T·M·C·Asser Press

Information Technology and Law Series IT&LAW 20

Innovating Government

Normative, Policy and Technological Dimensions of Modern Government

Simone van der Hof
Marga M. Groothuis *Editors*

Springer

Information Technology and Law Series

Volume 20

For further volumes:
http://www.springer.com/series/8857

Simone van der Hof · Marga M. Groothuis
Editors

Innovating Government

Normative, Policy and Technological Dimensions of Modern Government

T·M·C·Asser Press

Springer

Editors
Dr. S. van der Hof
Tilburg Institute for Law and Technology
Tilburg University
Warandelaan 2
5037 AB Tilburg
The Netherlands
e-mail: s.vdrhof@uvt.nl

Dr. M. M. Groothuis
Institute for Public Law
Leiden University
Steenschuur 25
2311 ES Leiden
The Netherlands
e-mail: m.m.groothuis@law.leidenuniv.nl

ISSN 1570-2782

ISBN 978-90-6704-730-2 e-ISBN 978-90-6704-731-9

DOI 10.1007/978-90-6704-731-9

Published by T.M.C. Asser press, The Hague, The Netherlands http://www.asserpress.nl

Produced and distributed for T.M.C. Asser press by Springer-Verlag Berlin Heidelberg

Cover design: eStudio Calamar, Berlin/figueres

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Series Information

The Information Technology and Law Series was an initiative of IT*e*R, the National programme for Information Technology and Law, which is a research programme set up by the Dutch Government and The Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995, IT*e*R has published all its research results in its own book series. In 2002, IT*e*R launched the present internationally orientated and English language *Information Technology and Law Series*. This series deals with the implications of information technology for legal systems and institutions. It is not restricted to publishing IT*e*R's research results. Hence, authors are invited and encouraged to submit their manuscripts for inclusion. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Contents

1 Innovating Government: An Introduction to the Book 1
Simone van der Hof

Part I Normative and Ethical Dimensions

2 Privacy 3.0 17
Anton Vedder

3 Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications 29
Irma van der Ploeg

4 Electronic Exchange of Signals on Youth at Risk: A Value Perspective 41
Ton Monasso

5 Regulating Invisible Harms 57
Noëmi Manders-Huits

Part II Policy Dimensions: Democracy

6 The Single Point of Failure 77
Beth Simone Noveck

7 Electronic Voting: Approaches, Strategies, and Policy Issues—A Report from Switzerland 101
Urs Gasser and Jan Gerlach

8 Striving Behind the Shadow: The Dawn of Spanish Politics 2.0 . . . 129
Ismael Peña-López

Part III Policy Dimensions: Surveillance

9 The Normality of Living in Surveillance Societies 151
David Murakami Wood and C. William R. Webster

10 The Evolution of New Technologies of Surveillance in Children's Services in England 165
Paul Michael Garrett

11 Electronic Child Records in The Netherlands: A Legitimate Path to Right Wrongs? 183
Simone van der Hof

12 Legitimacy Issues Regarding Citizen Surveillance: The Case of ANPR Technology in Dutch Policing 197
Charlotte van Ooijen

13 The Introduction of Biometrics in The Netherlands: An Evaluation under Data Protection and Administrative Law 217
Annemarie Sprokkereef

Part IV Legal Dimensions: EU Law Perspectives

14 The Use of Biometrics at the Borders: A European Policy and Law Perspective 231
Evelien Brouwer

15 Privacy and Data Protection Aspects of e-Government Identity Management 251
Brendan van Alsenoy, Els Kindt and Jos Dumortier

16 eHealth from a Dutch Perspective 283
Hilde van der Meer and Sjaak Nouwt

17 Implementation of the EU Services Directive: On eGovernment in a Decentralized Unitary State 315
Astrid M. M. van der Wijst and Marga M. Groothuis

18 The Impact of Europe on Geo-Information 329
Leo van der Wees

Part V Legal Dimensions: Techno-Legal Perspectives

19 Sharing Information between Government Agencies: Some Legal Challenges Associated with Semantic Interoperability 347
Dag Wiese Schartum

20 Public Information Infrastructures and Identity Fraud 363
Jan Grijpink

21 Access to Law in Europe 383
Laurens Mommers

Part VI Legal Dimensions: Law and Philosophy Perspective

22 Identity Theft and Fraud 401
Peter van Schijndel

Part VII Technological Dimensions

23 Biometrics and Smart Cards in Identity Management 419
Bart Jacobs and Erik Poll

24 How Devices Transform Voting 439
Wolter Pieters

Part VIII Synthesis

25 A Brave New Government? 455
Corien Prins and Wim Voermans

About the Authors

Brendan van Alsenoy obtained his law degree at the University of Antwerp in 2004. After completing his basic law studies, he obtained a degree of specialization in Human Rights at the Facultés Universitaires Saint-Louis, where he focused on Privacy Rights and Data Protection. In 2006, he graduated from the LL.M. program at Temple Beasley School of Law in Philadelphia. Brendan Van Alsenoy joined the Interdisciplinary Centre for Law and ICT of K.U. Leuven in March of 2007. His research has been focused on privacy, identity management, trust services, and digital evidence. He also pursues an interest in standardization initiatives in these areas, and is an active contributor to ISO/IEC JTC 1 SC 27/WG 5.

Evelien Brouwer is assistant professor at the Institute of Constitutional and Administrative Law of the Utrecht University. Her research interests include privacy and data protection law, human rights, and (European) migration law. Between 2002 and 2007, she was a researcher at the Centre for Migration Law at Radboud University Nijmegen where she defended her thesis Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System (Martinus Nijhoff Publishers, 2008).

Jos Dumortier is professor in Law and IT at the Faculty of Law at the Katholieke Universiteit Leuven. In 1990 he founded the Interdisciplinary Centre for Law and Information Technology and was its first Director. Since 1991 he has been active in lecturing, research, and consultancy in the area of Law and ICT. He is the editor of the International Encyclopedia of Cyber Law, and he regularly works as an expert for the Belgian federal and regional governments, the European Commission and several national and international organizations. He co-founded the IT law firm time.lex, of which he is currently a senior partner.

Paul Michael Garrett works in the School of Political Science and Sociology at the National University of Ireland, Galway. He is the author of three books critically examining social work with children and families: Remaking Social

Work with Children and Families (Routledge, 2003); Social Work with Irish Children and Families in Britain (Policy Press, 2004); 'Transforming' Children's Services? Social Work, Neoliberalism and the 'Modern' World (Open University/ McGraw Hill, 2009). His work has appeared in academic journals across a range of disciplines and he has presented papers at a number of international conferences. Paul is also a member of the Critical Social Policy editorial collective (where he is the Reviews Editor). Moreover, he is a member of the editorial board of the European Journal of Social Work and is a consulting editor for the US-based Journal of Progressive Human Services.

Urs Gasser is the Executive Director at the Berkman Center for Internet and Society at Harvard University. His research and teaching focus on information law and policy, and the interaction between law and innovation. Current research projects—several of them in collaboration with leading research institutions in the US, Europe, and Asia—explore policy and educational challenges for young Internet users, the regulation of digital media and technology (with emphasis on IP law), ICT interoperability, the institutional settings for fostering entrepreneurship, and the law's impact on innovation and risk in the ICT space. He has published and edited, respectively, seven books and has written over 60 articles in books, law reviews, and professional journals. Together with John Palfrey, he is the author of 'Born Digital: Understanding the First Generation of Digital Natives' (Basic Books, 2008). Previously, he served as the Faculty Director at the Research Center for Information Law at the University of St. Gallen (Switzerland), where he was an Associate Professor of Law.

Jan Gerlach is Executive Manager of the Research Center for Information Law at the University of St.Gallen, Switzerland. He holds an MA in Law and Economics. During his work as a research assistant, he has contributed to several different studies and reports in the field of information law. His research interests lie in topics related to the internet's interplay with society such as the conflicts between digitization and copyright, electronic democracy, political campaigns online, and the behavior of youth and young adults in social networks. Jan Gerlach is currently conducting research for his dissertation in the field of network regulation.

Jan Grijpink is Principal Adviser at the Dutch Ministry of Justice, with a special interest in strategic information issues. He studied Economics (1969) and Law (1971) at the University of Groningen and Organisation and Management (1976) at the Inter-University Institute SIOO in Utrecht. In 1997 he obtained his Ph.D. at the Technical University of Eindhoven based on his thesis on Chain-computerization. In 2004, he was appointed professor in Information Science (teaching Chain-computerization) at Utrecht University.

Marga M. Groothuis is assistant professor at the Faculty of Law of Leiden University in The Netherlands. She obtained her LL.M. at Queen Mary and Westfield College in London. From 2001 to 2005, she worked as a legal specialist at the Constitutional Affairs Department of the Dutch Ministry of the Interior. In 2004 Marga Groothuis obtained her Ph.D. for a thesis on legal aspects of automatic decision-making by government agencies. Her research currently focuses on legal aspects of eGovernment in Europe and on fundamental rights, and the rule of law in the digital age.

Simone van der Hof is associate professor at TILT (Tilburg Institute for Law, Technology and Society), Tilburg University, The Netherlands. In her research, she focuses (cf. I.174, 221, 337, 362) particularly on children, technologies, and regulation, dealing with the protection and empowerment of children in light of online risks, like cyberbullying and sexting, and the position of children in systems of surveillance. Other research interests include: social and legal issues in identity construction and identity management in electronic government. She has co-authored the book Framing Citizen's Identities—The Construction of Personal Identities in New Modes of Government (Wolf Legal Publishers, 2010).

Bart Jacobs is professor of Computer Security at the Radboud University Nijmegen. Earlier he worked in Cambridge, Utrecht, Amsterdam, and Eindhoven. Jacobs' research interest range from theoretical topics in mathematics and computer science to societal topics involving for instance privacy, e-ticketing, and e-voting. The author is co-founder of Digital Security group in Nijmegen that conducts research on software security, security protocols, applied cryptography, smartcards, and RFID. Apart from more fundamental research the group also carries out very applied security research—investigating the (in)security of particular systems—and has a strong interest in privacy.

Els Kindt studied Law and Philosophy at the K.U. Leuven Campus Kortrijk and graduated in Law from the K.U. Leuven in 1987. Thereafter, she obtained a Master of Laws in 1988 in the US. She is a member of the Brussels Bar and practised for 15 years until August 2003 as an attorney in the IP/IT Department of Linklaters (formerly De Bandt, van Hecke, Lagae) in Brussels. From the start, she specialized in Information Technology Law. Since December 1, 2003, she has been a contract legal researcher with ICRI with a focus on biometrics, identity management, and privacy law.

Noëmi Manders-Huits is assistant professor in applied ethics at Delft University of Technology. With a background in philosophy and business administration, she studies the ethical dimensions of new media and information technologies. She has particular interest in privacy and identity, ethics of technology, access to knowledge, and value-conscious design. In addition, she is Managing editor of the Springer-journal *Ethics and Information Technology*.

Hilde van der Meer is a health law advisor at the Royal Dutch Medical Association (KNMG), The Netherlands. At the KNMG, she is also the co-ordinator for foreign policy. On behalf of the KNMG, Hilde is a member of the Working Group on eHealth of the Standing Committee of European Doctors ('Comité Permanent des Médecins Européens, CPME').

Laurens Mommers graduated in Philosophy, Linguistics, and Law. He received his Ph.D. for a thesis on Applied Legal Epistemology. His research currently focuses on the accessibility of legal information, both on a technical, practical, and legal level. He is a consultant for Legal Intelligence, a Rotterdam-based company offering sophisticated search engines for the legal market.

Ton Monasso graduated from Delft University of Technology as a Master's of Science in System Engineering, Policy Analysis and Management. His master thesis researched policy considerations for information exchange around children with psychosocial problems. His chapter in this book partly builds on that thesis. Currently, he is working as senior consultant and researcher at Zenc, The Hague. His main interests are still in multi-actor cooperation and information exchange in the 'soft public sectors' such as education, youth care and health care. Ton frequently publishes on youth care, and IT. See http://www.tonmonasso.nl for an overview of his work.

David Murakami Wood is Canada Research Chair (Tier 2) in Surveillance Studies and Associate Professor in the Department of Sociology, Queen's University, Kingston, Ontario. He is the Managing Editor of Surveillance and Society, and a trustee of the Surveillance Studies Network (SSN). He is currently writing two books: Global Surveillance Societies (Palgrave, UK) and The Watched World (Rowman and Littlefield, USA).

Beth Simone Noveck is the United States Deputy Chief Technology Officer for open government. She directs the White House Open Government Initiative at http://www.whitehouse.gov/open. She is on leave as a professor of law and director of the Institute for Information Law and Policy at New York Law School and McClatchy visiting professor of communication at Stanford University. Dr. Noveck taught in the areas of intellectual property, technology, and first amendment law and founded the Law School's 'Do Tank' (dotank.nyls.edu), a legal and software R and D lab focused on developing technologies and policies to promote open government. Dr. Noveck is the author of Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful (Brookings Institution Press, 2009) and Editor of The State of Play: Law, Games and Virtual Worlds (NYU Press, 2006).

Sjaak Nouwt is a health law advisor at the Royal Dutch Medical Association (KNMG), The Netherlands, where he is dealing with legal issues of IT and eHealth, especially privacy and confidentiality. He is also a Honorary Fellow at TILT—Tilburg Institute for Law, Technology, and Society, Tilburg University. In 1997 he published his doctoral thesis on the use of information technology in health care and the protection of medical data.

Charlotte van Ooijen is a Ph.D. researcher at the Tilburg Institute for Law, Technology, and Society (TILT) and lecturer at the Tilburg School of Politics and Public Administration, both situated at Tilburg University, The Netherlands. She is also an expert in the Living in Surveillance Societies (LiSS) COST Action (http://www.liss-cost.eu). Her research interest concern technological surveillance, spatial information, public policy making, and legitimacy. In her dissertation she analyzes the implications of public surveillance of citizen mobility for the government-citizen relationship. Chapter 12 in this book, which describes the use of automatic number plate recognition (ANPR) by a Dutch police force, is a result of the first case study she conducted for her doctoral research.

Ismael Peña-López is a lecturer at the Open University of Catalonia, School of Law and Political Science. He holds a Ph.D. in the Information and Knowledge Society, a BSc in Economics, a MSc in Ecoaudit and Corporate Planning of the Environment and a post-degree in Knowledge Management. His main research interests are the barriers to adoption of ICTs (Digital Divide, e-Readiness, ICT4D) and how these technologies are having an impact in educational and political institutions: universities, schools, governments, parties, and nonprofits. He is editor of ICTlogy.net (ictlogy.net). Previous to his academic life, and for five years, he was Founding Member and later Director of the Development Cooperation Programme at the University, mainly working in e-learning for development and online volunteering.

Wolter Pieters (1978) is an interdisciplinary researcher in information security. After studying computer science and philosophy of science, technology and society, he wrote a Ph.D. thesis on electronic voting and worked for the Dutch Ministry of the Interior. Currently he coordinates the VISPER project on security in cloud computing at the University of Twente and organizes several events on the topic. He has published on electronic voting, verification of security properties, access control, and philosophy and ethics of information security.

Irma van der Ploeg (1964) holds degrees in philosophy and science and technology studies. In 2006 she was appointed as Associate Professor of Infonomics and New Media at Zuyd University, Maastricht/Heerlen, The

Netherlands, where she is heading the Infonomics and New Media Research Centre (infonomie.hszuyd.nl). She has published extensively on philosophical, normative, and gender aspects of medical technologies and information technologies, in particular on biometric identification technologies. She is author of The Machine-Readable Body: Essays on Biometrics and the Informatization of the Body (Maastricht: Shaker, 2005). In 2008 she was awarded a Starting Grant for Independent Researchers from the European Research Council, for a large, 5-year research project entitled Social and Ethical Aspects of Digital Identities. Towards a Value Sensitive Identity Management (http://www.digideas.nl).

Erik Poll is associate professor at the Radboud University. Earlier he worked at the Eindhoven University of Technology, INRIA in France, and the University of Kent in England. His research interest include formal specification and verification, programming languages, and smartcards. The author is co-founder of Digital Security group in Nijmegen that conducts research on software security, security protocols, applied cryptography, smartcards, and RFID. Apart from more fundamental research, the group also carries out very applied security research—investigating the (in)security of particular systems—and has a strong interest in privacy.

Corien Prins is professor of Law and Informatization at Tilburg University, Institute for Law, Technology, and Society (TILT). She combines this position with being a member of the Dutch Scientific Council for Government Policy (WRR) in The Hague. Corien Prins holds a degree in law as well as Slavic languages and literature from Leiden University, The Netherlands. She headed the Research Institute TILT from 1996 to 2008. Corien Prins is a member of the Royal Netherlands Academy of Arts and Sciences (KNAW). Her present research topics include (international) regulatory questions of ICT and new technologies (biotechnology, ambient intelligence, nanotechnology), commodification and propertization of information, consumer protection in an ICT-society, biometric technology, e-government, NGO's and new technologies, privacy and anonymity, identity management, identity theft/fraud, and on-line personalization.

Dag Wiese Schartum Doctor of Law 1993, Professor at Norwegian Research Center for Computers and Law (NRCCL) 1997, Director of NRCCL since 2007. Schartum's research is mainly within the areas of data protection and information security, eGovernment, automated decision-making, and ICT-tools for lawyers.

Peter van Schijndel is a lawyer. Peter was a researcher at the Centre for eLaw at Leiden University, focussing on the concept of identity (theft). Currently, Peter is affiliated with the centre as an external Ph.D. candidate.

Annemarie Sprokkereef is a social studies teacher at Lorentz Lyceum, Arnhem, and Associate Fellow at the Tilburg Institute for Law and Technology (TILT),

University of Tilburg, The Netherlands. A political scientist and former police officer, Annemarie has published extensively on the regulation of biometrics. She has been involved in different European research networks, including FIDIS (Future of Identity in the information Society) and BEST (Biometric European Stakeholders Network) and sits on the Ethical and Dual Use Advisory Board of the ADABTS consortium (Automatic Detection of Abnormal Behavior and Threats in crowded Spaces).

Anton Vedder is affiliated to TILT, The Tilburg Institute of Law, Technology, and Society of the Law School of Tilburg University. His primary research interests are concerned with ethics and the regulation of innovative technologies. He is especially interested in the interplay between technological developments and the conceptualization of basic moral and legal notions. Recent publications include articles and books on cognitive enhancement, ambient technology and autonomy, privacy versus public security issues, ethical and regulatory aspects of knowledge discovery in databases, responsibilities related to innovative technologies, quality of information, and credibility of experts, security of communication, and the legitimacy of regulatory arrangements using technology.

Wim Voermans is professor of Constitutional and Administrative law at Leiden University. Voermans current research focuses on Dutch and European constitutional law, with a particular interest in the Dutch and European legislature. Focal points in his recent research are: comparative research on IT use in legislative procedures and processes, quality of (EU) legislation, transparency of legislative procedure, institutional balance, consultation, simplification, red tape reduction, transposition and implementation of EU legislation, compliance and enforcement and legislative evaluation. Voermans is currently working in the Legis project of the Dutch Government, a project attempting to improve the overall transparency and efficiency of the Dutch legislative process.

C. William R. Webster is a Senior Lecturer in Public Management at the Stirling Management School, University of Stirling, Scotland (http://www.management.stir.ac.uk). He is Programme Director of the MBA in Public Service Management and Chair of the Living in Surveillance Societies (LiSS) COST Action. LiSS is a 4 year FP7 funded European research programme, exploring the normality of life surrounded by rapidly increasing levels of technologically mediated surveillance (http://www.liss-cost.eu). William's research interests are broadly in the areas of contemporary public policy and management, and the policy processes and governance structures associated with governing in the information age. More specifically, his research interests include; the governance structures surrounding the use of new Closed Circuit Television (CCTV) surveillance systems in public places, the emergence of technologically mediated surveillance practices and their regulation, and the development of innovative electronic public services, citizenship and democracy (e-Government).

Leo van der Wees studied Law at Leiden University where he specialized in ICT and Law. After the completion of his studies he worked as a computer programmer. He then pursued his career at Erasmus University in Rotterdam where he worked as a researcher. Now Van der Wees is researcher at the Tilburg Institute for Law, Technology, and Society. Next, he works as chief executive officer at Recht.nl, a Dutch internet portal for lawyers, and for the Dutch foundation RechtenOnline. The latter organization provides and promotes ICT services in Dutch legal education.

Astrid van der Wijst is legal advisor at the Environmental Protection Agency of the local and regional authorities operating in the area West-Holland, The Netherlands. Until recently she worked as a consultant at NL Agency which is a Department of the Dutch Ministry of Economic Affairs that implements government policy for sustainability, innovation, and international business and cooperation.

Chapter 1
Innovating Government: An Introduction to the Book

Simone van der Hof

Abbreviations

ANPR	Automatic number plate recognition
EU	European Union
ICT	Information and communication technology
IDM	Identity management
IMIS	Internal market information system
RFID	Radio frequency identification
VSD	Value-sensitive design

Contents

1.1 Background—the Tale of Reinventing and Innovating Government 2
1.2 Crossing Borders in Studying and Designing New Modes of Government 4
1.2.1 Crossing State Borders 4
1.2.2 Crossing Disciplinary Borders 5
1.2.3 Crossing Policy Borders 5

Contribution received in 2010.

The first part of this chapter is based on research published in Van der Hof et al. 2009.

S. van der Hof (✉)
TILT – Tilburg Institute for Law, Technology and Society, Tilburg University, Tilburg, The Netherlands
e-mail: hof@tilburguniversity.edu

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_1,

1.3 Structure of the Book—Various Dimensions 6
1.4 Normative and Ethical Dimensions—Part I 6
1.5 Policy Dimensions—Parts II and III 8
1.5.1 Democracy 8
1.5.2 Surveillance 9
1.6 Legal Dimensions—Parts IV, V and VI 10
1.6.1 EU Law Perspectives 10
1.6.2 Techno-legal Perspectives 12
1.6.3 Law and Philosophy Perspective 13
1.7 Technological Dimensions—Part VII 13
References 14

1.1 Background—the Tale of Reinventing and Innovating Government

The narratives in this book can be positioned against a background of a rapidly changing societal and policy landscape, both empirically and theoretically, in light of turbulent technological developments and new social paradigms. Since the mid-1990s, many Western governments have 'embraced the idea that new technologies might be exploited to "reinvent" their own activities' (Bellamy and Taylor 1998). Hence, fueling the new paradigm of the reinvented government, as elaborately considered by Osborne and Gaebler (1992), under the New Public Management philosophy, and rendering notions of business-like and customer-driven government which are facilitated by the introduction of ICTs in public administration and a growing interconnectivity of public organizations and policy spheres. Since then we have seen transformations in many areas of public administration under the heading of electronic government or e-government.

Electronic government denotes the implementation of information and communication technologies to facilitate or improve the delivery of public services to citizens and companies. Consequently, the focus of electronic government is particularly centered on the digitization of transactions between governments and citizens or business. Electronic government is part and parcel of the transition from modern society to an information society or in Castells (1996) terms an 'informational society.' This marks the shift away from the nineteenth century industrial society because halfway during the nineteenth century, information and data became the primary raw materials of Western economies. Obviously, information is now an important 'source of productivity and power' (Castells 1996, p. 21) for governments. Technological innovations have promoted information processing opportunities in the public sector and affected many aspects of public administration, e.g., relations between the state and citizens, policy making, law enforcement, etc. and also democratic processes, like e-voting.

The progress of electronic government has been immensely aided by the ever-growing capacities for storing data and processing data through broadband technology and is also due to the fact that most people have access to the Internet

nowadays. Further innovations in e-government are emerging as a result of all kinds of mobile devices, such as smart phones, and other technologies, smart cards, RFID, NFC, and biometric technologies, that allow new applications to foster communication between citizens and the state or to deliver public services. In the near future, it is expected that these technologies will become part of smart environments, also referred to as 'ambient intelligence' (van den Berg 2009) and 'Internet of things' (van Kranenburg 2008), and will eventually completely change the fabric of our societies. In these smart environments context-aware, adaptive, and invisible technologies continuously anticipate the needs and preferences of citizens, and personalize public services accordingly. Although, the development of such smart environments is still at an early stage, some complex new questions and problems in respect of them have already been identified or are anticipated (SWAMI 2006), besides other vulnerabilities that are presently increasing extensively as a result of a growing data intensity and digitization, like identity fraud, information security and data breach incidents.

Notwithstanding these risks, new technologies also raise abundant opportunities to redesign the interaction between citizens and the state. ICTs can encourage e-participation of citizens by introducing Web 2.0 tools (like wikis, chat, blogs, social networking sites, online fora, e-petitions, serious gaming etc.).[1] Or (collectives of) citizens themselves take up these technologies so that they can be more involved in public administration and political processes in which they have an interest or can provide certain expertise. There seems to be a growing citizen involvement through ICTs. Citizens are becoming increasingly articulate and knowledgeable about public policy matters of health, education, etc., and how to perform public tasks (Leadbeater and Cottam 2007). Some expect this to foster the democratization of relations between citizens and the state by achieving more trust and transparency, greater active involvement of citizens in democratic processes, and empowerment of citizens. Others take a more skeptical stance and think trust will not increase and motivation amongst citizens to participate is mostly lacking (see Frissen et al. 2008).

Beyond e-government and against the backdrop of technological innovation by governments more generally, we can observe a transition in which the relevance of data as an important 'source of productivity and power' is considerably on the increase and developments go beyond the transactional and interactional focus that is particularly characteristic of e-government or government 2.0 initiatives. The technological mediation of relations between the state and its citizens becomes more and more sophisticated, ubiquitous and, at the same time asymmetrical or one could even say disproportionate. This tendency is typical of modern Western society in which security, safety, and control are key and there is a strong belief in the ability of state policy to re-engineer society such that social problems disappear (see Beck 1994; Giddens 1998; Scientific Council for Government Policy 2008). This tendency entails a culture of control in which prevention and risk

[1] Frissen et al. 2008 uses the term user-generated state to indicate such developments.

anticipation become key objectives of public policy (Garland 2001), fueling technological innovation and data intensity, which denotes the trend of the state collecting, classifying, and using tremendous amounts of (new kinds of) (personal) data in hundreds of—often interconnected—databases, in many policy spheres in order to enable these objectives and resulting in what is called a surveillance society (Lyon 2001).

The innovation of government ultimately transcends the mere introduction of technologies in state policy and practice and any contemplation of developments in this respect must go beyond a predominantly instrumental view and acknowledge the fact that we are in the middle of complex societal processes, twinned with a great variety of important ethical, legal, social, and political questions that eventually also impinge on fundamental societal issues, like immigration, poverty prevention, and minority empowerment, and demand a more holistic outlook on—acceptable—directions of developments and their—potential—outcomes. The issues recounted in this book allow us a glance at the complexity of modern government and show the highly dynamic area, in which multiple interpretations and approaches may be determined with respect to the ways in which ICTs can be implemented and used by the state and how they impact on, for instance, civil liberties and more generally the relations between nation states and its citizens. Ultimately these developments and the choices made in respect of them substantially mold the societies that we have to live in and are therefore in dire need of meticulous and critical scrutiny, in respect of which this book aims to provide a humble yet valuable contribution.

1.2 Crossing Borders in Studying and Designing New Modes of Government

The aim of this book has been to relate a diversity of views of relevant and persistent issues with respect to modern government and the use of new technologies from a diversity of perspectives and in various domains. In a sense, you could say that the articles in this book cross borders in three distinct ways in order to provide a varied picture of some of the issues at hand.

1.2.1 Crossing State Borders

Several chapters in the book take a top-down approach while others more deal with questions in a bottom-up or a combined approach. A top-down approach means that the perspective of the European Union (EU), most notably EU legislation and policy, is taken as the starting point for conveying information, ideas, and opinions to the reader. EU policy and regulation shape these national systems in a top-down

way. Since EU regulation has extensively permeated national legal systems of the Member States, it is particularly relevant to many issues (privacy, biometrics, identity management, e-health, geo-information, cross-border public services, access to law) discussed in this book.

At the same time, we see developments in nation states with a—sometimes culturally defined—dynamics of their own, albeit still framed by EU regulation as far as EU member states are concerned. These developments can perhaps provide insights or lessons to policymakers in other countries or highlight fundamental questions that are raised as well as directions on how to address these questions. Hence, some of the chapters also or exclusively address national circumstances and outlooks or present national case studies in particular policy domains or other relevant areas, like e-health, e-youth, collaborative democracy, e-voting, politics 2.0, surveillance, modern policing, interoperability, access to law, and identity fraud.

1.2.2 Crossing Disciplinary Borders

In modern times the state is faced with a multiplicity of complex social, political, cultural, or technological challenges that profoundly impact issues of governance. Given that modern society becomes more and more complicated and hence raises increasingly complex questions, it is imperative that experts from multiple disciplinary backgrounds are involved in addressing these challenges for today's nation states. For precisely these reasons, also in academia, the growing importance of multidisciplinary perspectives can be observed within separate research projects—albeit sometimes perhaps reluctantly and not without difficulties given the distinctive mono-disciplinary cultures.

By joining authors from a diversity of backgrounds (ethics, law, public administration, political science, sociology, communications science, information science, and computer science) in one book, readers (academics, policy makers, etc.) are confronted with a variety of disciplinary perspectives on persistent themes and issues, like privacy, biometrics, surveillance, democracy, electronic government, electronic voting, and identity management, that are central to today's evolution of new modes of modern government. The aim is not to provide an integrated theoretical—interdisciplinary—perspective on the various themes, although in some respects it is apparent that some of them, for instance biometrics, surveillance, and identity (management), show rather natural, even inevitable cross-overs from one to another discipline.

1.2.3 Crossing Policy Borders

Several chapters in this book address issues and developments in specific policy domains, such as health care, youth care, policing, and immigration. What all of these domains have in common is that they experience the impact of

technologization of information processes and an increasing technological mediation of relationships therein. Although each domain raises characteristic challenges depending on the social or political issues at hand and, particular interests that are involved in public policy-making and administrative processes, clearly there are also persistent challenges or questions across these policy domains. Hence, several overarching themes can be identified across this book, like surveillance and democracy, and some of the chapters particularly scrutinize more general themes, like identity fraud, biometrics, interoperability, identity management, chain computerization, access to public sector information, though from specific points of view or disciplinary perspectives.

1.3 Structure of the Book—Various Dimensions

The various themes and disciplinary perspectives of the book have been structured across four prevalent dimensions. These dimensions are

Normative and ethical dimensions—Part I;
Policy dimensions—Parts II and III;
Legal dimensions—Parts IV, V and VI;
Technological dimensions—Part VII.

In the following sections, the various themes analyzed by the authors within these four dimensions will be expounded briefly in order to provide an overview of the setup and an introduction into the contents of the book that can function as a roadmap for readers. In addition, the book is ended with a Chap. 25 by Corien Prins and Wim Voermans which provides a synthesis of a variety of important observations based on the contributions by the other authors in this book.

1.4 Normative and Ethical Dimensions—Part I

In Chap. 2 entitled 'Privacy 3.0', Anton Vedder scrutinizes the public debate and theoretical controversies concerning privacy to show how privacy, as a value, pertains to new technological developments and changing social relations. In his view, the public debate suffers from a superficiality where privacy is concerned and this is sharply contrasted by the fundamental scholarly recourse on privacy, which historically manifests a richness of views and controversies amongst legal theorists and ethicists. He presents us with a historical overview of these theoretical controversies on privacy (as a value) to, accordingly, demonstrate how the social debate can benefit from their insights in light of cutting edge developments in the area of ambient intelligence and converging technologies that are expected to radically change society. Vedder stresses the importance of augmenting social debate with theoretical acumen in order to better grasp the complexity of

protecting the underlying values (i.e., autonomy, welfare, equality, justice, dignity, status, and tranquillity) which are at stake and to resolve, or at least contend normative issues in respect of privacy and novel technological developments in a well-reasoned way.

In Chap. 3 on 'Normative assumptions in biometrics: on bodily differences and automated classifications', Irma van der Ploeg calls our attention to ways in which bodily differences can fundamentally impact the lives of individuals as a result of improbable normative assumptions pertaining to the use of biometric technologies. First, she explains how assumptions of similarity (each individual is assumed to have particular features that are crucial to the functioning of biometric technologies), stability (biometric features do not change over time), and availability (visibility and touchability of biometric features in ways demanded by biometric systems) are central to biometric systems, and how they fail and lead to exclusion of individuals. Second, van der Ploeg critically considers developments in soft biometrics, i.e., biometric applications using 'partial identities' and general body characteristics such as body weight, gender, age, or ethnicity. She particularly finds the enhanced, inherent classification capabilities based on, e.g., gender, age, and ethnicity worrisome because they can potentially lead to situations where individuals are unjustly discriminated against by automated and non-transparent systems. According to her, both concerns require ongoing critical research and assessment.

Ton Monasso in his chapter 'Electronic exchange of signals on youth at risk—a value perspective' (Chap. 4) makes a strong case for incorporating values into the design of information systems (value-sensitive design or VSD) by analyzing a Dutch youth care risk-signaling system. He sets out by explaining the role of designers in influencing the technology which is inclined to become more autonomous over time, and how values and technology can be conjoined methodologically through what he calls Groenewegen's framework. Based on this methodology, trade-offs between various values (like the successful development of children, moral autonomy, and the absence of information abuse) can be made in system's design. The eventual impact on values is thereby not merely determined by the technology, but also depends on the particular social and institutional contexts, and the methodology, as Monasso shows, therefore allowing to approach systems design from the interdisciplinary perspective necessary for VSD.

In 'Regulating invisible harms' (Chap. 5), Noëmie Manders-Huits delves into the potential harms pertaining to identity management (IDM) for e-government by adapting Joel Feinberg's concept of 'accumulative harm' to this particular context. First, by reference to Goldman's criteria of power, fecundity, speed, efficiency, and reliability she argues that IDM has obvious advantages. However, there are also various sorts of potential harms involved in IDM, one of which is what she calls accumulative informational harm, defined as 'potential harm created by the accumulation of multiple bits of sometimes seemingly innocent bits of (identity related) data.' Informational accumulative harm can impact individuals (improper treatment as a result of incorrect data or profiles), groups (unfair exclusion of groups of individuals) and society (shifting power balance between citizens and

the state). Manders-Huits argues for the prevention of accumulative informational harm through VSD and puts forward the principle of minimalism as key to the design of IDM systems.

1.5 Policy Dimensions—Parts II and III

The policy dimensions addressed in this book have been arranged in two prominent themes, i.e., democracy and surveillance.

1.5.1 Democracy

In her chapter 'The single point of failure' (Chap. 6), Beth Simone Noveck takes position against the prevailing idea that government professionals are better suited than citizens to take informed public decisions on complex policy matters. Concentrating decision-making powers in the hands of a few government professionals, legislators, civil servants, etc., creates what she calls the single point of failure. As a result, decisions are inadequate and a lack of accountability and transparency in decision-making emerges, all of which may lead to a lack of legitimacy and trust in government. Civic society, however, increasingly embraces new technologies to unfold collective action, disconnected from government, with opportunities to amend the single point of failure by augmenting transparency and creatively innovating collaboration amongst experts or ordinary people. Noveck makes a case for an open and collaborative democracy in which new social and visual technologies facilitate networked publics to make adequate public decisions, illustrated by, for instance, emerging Peer-to-Patent practices.

In 'Electronic voting: approaches, strategies, and policy issues—a report from Switzerland' (Chap. 7), Urs Gasser and Jan Gerlach render insights from three Swiss pilot projects on e-voting which were conducted in a decentralized and distributed way but, at the same time, contribute to a national strategy on e-voting. The authors have comprehensively presented the opportunities and challenges of these initiatives from a public policy, regulatory, and design perspective. Thus they show the many complexities of implementing and using e-voting systems, which include legal, technological, social, and political challenges. Some of these challenges are not qualitatively new but have become more prominent with e-voting and occur on a larger scale than with traditional voting. The authors note that there are ways to address these issues by combining various—legal, technological, and social—modes of regulation and they point out that e-voting shows great promise in terms of increased autonomy, and—potentially—enhanced participation and quality.

In Chap. 8 named 'Striving behind the shadow—the dawn of Spanish politics 2.0', Ismaël Peña-Lopez critically explores the (lack of) uptake of web 2.0 technologies in Spanish public debate, campaigning, and political elections. The slow

uptake in Spanish politics 2.0 is partly due to e-readiness not being as high in Spain as for example in the United States; however, according to the author, other reasons lie in the fact that Spaniards have a strong trust in institutions, and participation on a more horizontal level is thus low. In addition, some political parties do not have enough funds to partake in 2.0 initiatives. Peña-Lopez also points to a digital divide. The educated, tech-savvy, and politically critical citizens are much more active in online politics. Although overall a networked political ecosystem with open and innovative interactions between politicians and citizens has not (yet) emerged, Peña-Lopez presents some promising initiatives that can feed optimism concerning Spanish politics 2.0.

1.5.2 Surveillance

David Murakami Wood and William Webster begin with a chapter on 'The normality of living in surveillance societies' (Chap. 9) in which they argue 'that technologically mediated surveillance is becoming normalized across Europe and that this is altering the landscape of liberty, security, and citizen-state relations.' The normality (as opposed to the emergence) of living in surveillance societies should, in their view, be the starting point for meticulously contemplating ethical and political implications for societies and their people. Given the multi-dimensional nature of surveillance, which is summed up by the authors as subtle, normal, ubiquitous, deep, unobtrusive, and powerful, it is high time to thoroughly investigate how living and working in a 'surveillance society' really impacts our lives and institutions in order to properly understand and assess the consequences of modern surveillance.

In 'The evolution of new technologies of surveillance in children's services in England' (Chap. 10), Paul Michael Garrett elaborates the issues of state surveillance from the perspective of youth care in the UK, where increasingly a whole range of surveillance technologies—telecommunications, video surveillance, the database, biometrics and locating, tracking, and tagging technologies—are used in youth care, despite fundamental concerns like function creep, normalization of pervasive surveillance, democratic legitimacy, transparency, and accountability. Garrett describes how the case of ContactPoint, an enhanced universal child monitoring system developed by the UK government, was critically received by politicians and a diversity of organizations and how, in turn, the then UK government had tried to take the heat out of this controversial matter by technologizing arguments.

In Chap. 11, entitled 'Electronic child records in the Netherlands—a legitimate path to right wrongs?', Simone van der Hof explores a similar development, i.e., Electronic child records, in the Netherlands from the perspective of a rights-based approach and good governance principles. A trend emerges to develop mere digitized records of children in youth healthcare into ubiquitous and multipurpose monitoring systems for the broader youth care domain to generate complete pictures of every child in the Netherlands. So far, the problematic elements of such a system—like function creep, stereotyping, care avoidance, professional autonomy,

and information security—are not or hardly considered by government agencies involved. van der Hof contends how this development does not always sit well with promoting the best interest of the child from a rights perspective. Additionally, the state does not properly live up to administrative principles under the rule of law. Respecting human rights and fundamental principles, the state should give due attention to child rights and show due care in designing a system that may deeply affect human lives.

Charlotte van Ooijen then moves the focus toward innovations in policing in 'Legitimacy issues regarding citizen surveillance—the case of ANPR-technology in Dutch policing' (Chap. 12). She concentrates on dilemmas of legitimacy in practices of nodal policing, i.e., the policing strategy focused on surveillance of infrastructures. ANPR—automatic number plate recognition—is a powerful tool given that it allows the police to collect data for future investigations and detect patterns of (potential) criminal activity. Research done by Ooijen reveals that although the police is sensitive to issues of legitimacy of ANPR practices, this is so, for mere pragmatic reasons. Increased effectiveness and efficiency are key to modern police policy and perceived to legitimatize ANPR usage, even if the required legal rules are absent, and to legitimatize the police organization per se.

Annemarie Sprokkereef focuses on 'The introduction of biometrics in the Netherlands—an evaluation under data protection and administrative law' (Chap. 13). In her contribution she describes the emergence of biometric technologies and applications in the public and the private sector. Then she focuses on the unintended side-effects of government biometrics policy, which in itself lacks a comprehensive view on the deployment of biometrics by the Dutch government, and points at the considerable gaps in knowledge and impact assessment in the public sector. Moreover, civil liberties have been disregarded in the quest for efficiency and national security. The influence of both the Dutch Data Protection Act and the Data Protection Authority as enforcer of the Act is very limited. The lack of policy coherence and citizen protection is contrary to the requirements set by the principles of proper administration.

1.6 Legal Dimensions—Parts IV, V and VI

These parts of the book provide three angles on legal dimensions in new modes of government, i.e., EU law perspectives, techno-legal perspectives, and a law and philosophy perspective.

1.6.1 EU Law Perspectives

In the first part on EU law perspectives, Evelien Brouwer commences with an analysis of the large-scale use and centralized storage of biometrics against the backdrop of privacy and data protection law in her chapter entitled 'The use of

biometrics at the borders—a European policy and law perspective' (Chap. 14). She shows how tools for immigration control, such as large-scale databases (including biometric data), like Eurodac, Visa Information System, and Schengen Information System II, are increasingly being deployed for law enforcement and national security purposes. However, pursuant to the rights to private life (Art. 8 ECHR) and data protection as well as recent case law (*Marper* v. *UK*) these measures can contend to be disproportional and in conflict with the purpose limitation principle. Moreover, contrary to what the European Commission says, in case of EURODACT, there is no evidence of the effectiveness and necessity of these measures for law enforcement despite an extensive privacy impact assessment.

Next is Chap. 15, 'Privacy and data protection aspects of e-government identity management' by Els Kindt and Brendan Van Alsenoy. The authors provide an analysis of how data-protection principles apply to e-government and particularly identity management. They explore current practices in relation to these principles in two specific cases, i.e., the internal market information system (IMIS) and applications that use biometric identifiers and identify various recurring challenges in this respect, like legitimacy of processing, determination of roles and responsibilities, re-purposing of personal data, and transparency in processing personal data. The IMIS case shows a diverse picture with data protection rights in some instances being accommodated, but also providing examples of situations in which a comprehensive approach towards these principles is missing. In biometrics, considerations of efficiency rather data protection principles lead the way in designing applications and a specific regulatory framework is lacking in most Member States.

Sjaak Nouwt and Hilde van der Meer address legal issues pertaining to eHealth developments in 'eHealth from a Dutch perspective' (Chap. 16). They present an overview of eHealth policy developments in the European Union and explore various recent Dutch eHealth initiatives, which become increasingly important in an aging society in which chronic diseases expand. Legal certainty is crucial in encouraging e-health innovations, particularly in light of e-health services (potentially) being provided in cross-border settings. However, the e-health legal landscape is comprised of a variety of legal fields—such as privacy and data protection law, competition law, contract law, product liability law, health care law—which makes it quite complex. In the authors' view e-health issues are too diverse to allow for a general e-health law, but national and—in certain respects—EU coordination could clarify e-health law and policy, and encourage developments in this field.

In 'Implementation of the EU Services Directive in the Netherlands: on eGovernment in a decentralized unitary state' (Chap. 17), Marga Groothuis and Astrid van der Wijst analyze the impact of the EU Services Directive on the legal framework for eGovernment in a decentralized unitary state like the Netherlands. This Directive imposes an obligation on the Member States to set up a digital Point of Single Contact, through which service providers can complete legal formalities electronically. The authors investigate the extent to which the concept of 'Point of Single Contact' fits into the Dutch constitutional framework.

They show that there remains a tension between, on the one hand, the principle of respect for the allocation of functions among relevant competent authorities at the national, regional and local level, and on the other hand the creation of the Point of Single Contact. Furthermore, they provide an analysis of the digital Point of Contact under the general principles of good governance, such as legality and reliability.

Leo van der Wees addresses the effect of EU law and policy on re-use of geo-information, potentially leading to technological innovations, in his chapter entitled 'The impact of Europe on geo-information' (Chap. 18). van der Wees explains the role of several EU directives (database protection, re-use of public sector information, INSPIRE) and assesses how they have or have not contributed to the availability and re-use of geo data. Moreover, he reflects on the Dutch *Landmark* case where the court decided that both database protection rights and re-use rules do not apply to government databases, thus positively influencing the availability of geo data. In retrospect, EU directives seem to have inspired a change in the mindset of policy makers given that cautiously geo-information is released under more favorable terms to allow for commercial exploitation of geo-information.

1.6.2 Techno-legal Perspectives

In the part on techno-legal perspectives, Dag Wiese Schartum opens in Chap. 19 with 'Sharing information between government agencies—some legal challenges associated with semantic interoperability' where he unfolds the tension between 'the rather flexible, open and discretionary legal system, and the rather formalized, closed, and inflexible computerized information systems.' Schartum analyzes how various kinds of legal concepts, i.e., local, regional, and global, function in light of semantic operability, taking the 'live-in partner' concept to illustrate the complexity of seemingly simple terms. Schartum offers strategies to accommodate vagueness and formalization, particularly making a case for the use of a framework of basic definitions each of which allows for adding particular elements when opportune in light of political considerations.

Next the Chap. 20 called 'Public information infrastructures and identity fraud' by Jan Grijpink, he inquires into issues of chain computerization and identity fraud in the criminal law enforcement. Grijpink explains how the doctrine of chain computerization offers remedies for what the author terms 'fallacies of the wrong level' (unexpected negative results due to scale size) in the development of extensive chain information systems. He then ascertains how identity fraud is used by criminals in national and international chain information systems to escape from serving prison sentences or building a criminal record. In order to alleviate these problems, particularly in view of the emerging large-scale cross-border information systems, Grijpink proposes strategies and particular measures, like remote biometric verification, to counter identity fraud in law enforcement and other areas.

In 'Access to law in Europe' (Chap. 21), Laurens Mommers translates the promise of online availability of legal information, like legislation, parliamentary proceedings, and case law, into consecutive levels of accessibility—primary, secondary, and tertiary—with mounting functionalities and thus usefulness for citizens, and studies if and how in two cases (EUR-Lex and the Dutch official gazette website officielebekendmakingen.nl) these levels have been designed. Subsequently, Mommers argues for a right of access to legal information, i.e., a right to be able to notice and understand legal information using, for example, the 'average citizen' as the fixed point, to make a strong case for enhanced (tertiary), accessibility (meaningful access and understandability) of such information.

1.6.3 Law and Philosophy Perspective

A law and philosophy perspective on identity and identity-related crime is provided by Peter van Schijndel in 'Identity theft and fraud' (Chap. 22). Building on the concept of the 'external identity' that denotes the trend of identity playing an increasingly important role in our interactions with the state, the author analyzes how and why an individual's identity may be abused, and whether the law provides adequate solutions against identity theft or identity fraud. Given that—unlike, e.g., the US—the Netherlands has not criminalized such abuses per se, we have to adhere to other, less appropriate provisions concerning such crimes as fraud and theft. Describing the Dutch *Kowsoleea* case, van Schijndel reveals the severity of the consequences that identity theft may come to as well as how the state can fail in making amends towards its citizens. According to the author, future legislation should focus on the externalized identity and particularly provide preventative measures.

1.7 Technological Dimensions—Part VII

In the seventh part of the book, Bart Jacobs and Erik Poll delve into the biometric and smart card technologies used in modern passports and deal with issues of security, power imbalance, and privacy ('Biometrics and smart cards in identity management', Chap. 23). They set out to explain in detail the operational side, shortcomings, and risks of smart card, biometric, and RFID technologies, all which are part of e-passports. They point out where the security of these technologies is in need of improvement or how (extra) security can infringe on the privacy of citizens. The use of biometrics and smart cards has in itself also privacy implications in terms of surveillance that shifts the power balance between citizens and the state towards the latter. The state is advised to take more time for reflection in order to avoid mistakes when introducing such technologies in society.

In Chap. 24, 'How devices transform voting', Wolter Pieters contemplates the challenges for electronic voting from the perspective of philosophy of technology.

Setting out with an historical account on how electronic voting has, for the time being, been upstaged by a pressure group called We Don't Trust Voting Computers, the author draws our attention to the notion of implicit requirements in technological mediation and its relevance in shunning unwanted side-effects of technology as occurred with electronic voting in respect of verifiability and secrecy of casted votes. He shows how technological mediation can influence voting at the micro, meso, and macro level, what challenges rise for the voting system, voter autonomy, secrecy and privacy, and verifiability, and, with the example of Estonia, what subtle conceptual shifts can ensue with electronic voting.

References

Beck U (1994) The reinvention of politics, towards a theory of reflexive modernization. In: Beck U, Giddens A, Lash S (eds) Reflexive modernization. Polity Press, Cambridge

Bellamy C, Taylor J (1998) Governing in the information age. Open University Press, Buckingham/Philadelphia

Castells M (1996) The rise of the network society. Blackwell Publishers, Oxford

Frissen V et al (2008) Naar een 'User Generated State'? De impact van nieuwe media voor overheid en openbaar bestuur. TNO/Ministry of the Interior and Kingdom relations

Garland D (2001) The culture of control, crime and social order in contemporary society. Oxford University Press, Oxford

Giddens A (1998) Risk society, the context of british politics. In: Franklin J (ed) The politics of risk society. Polity Press, Cambridge, pp 23–34

Leadbeater C, Cottam H (2007) The user generated state: public services 2.0. In: Diamond P (ed) Public matters: the renewal of the public realm, public service reform group http://www.charlesleadbeater.net/archive/public-services-20.aspx

Lyon D (2001) Surveillance society, monitoring everyday life. Open University Press, Buckingham (issues in Society series)

Scientific Council for Government Policy [Wetenschappelijke Raad voor het Regeringsbeleid] (2008) Onzekere veiligheid [Uncertain security]. The Hague, Oct 2008

SWAMI (Safeguards in a World of Ambient Intelligence) (2006) Deliverable D2, dark scenarios in ambient intelligence: highlighting risks and vulnerabilities. Jan 2006

van den Berg B (2009) The situated self, identity in a world of ambient intelligence. Dissertation

van der Hof S, Leenes RE, Fennell S (2009) Framing citizen's identities, the construction of personal identities in new modes of government in the Netherlands. Research commissioned by the Netherlands Organization for Scientific Research, Tilburg University, p 266

van Kranenburg R (2008) The internet of things. A critique of ambient technology and the all-seeing network of RFID. Amsterdam. http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf

Part I
Normative and Ethical Dimensions

Chapter 2
Privacy 3.0

Anton Vedder

Contents

2.1 Introduction 17
2.2 The Public Debate 18
2.3 The Meaning of Privacy as a State of Affairs 19
2.4 The Meaning of Privacy as a Value 22
2.5 Normative Impact of Ambient Intelligence and Converging Technologies 23
2.6 Conclusion 25
References 26

2.1 Introduction

'Dead or as good as dead.' Not so long ago articles and essays on privacy often started with a statement like this one. Unfortunately, those announcing the end of privacy often did not indicate what exactly was going on. Is our privacy indeed coming to an end? Can we no longer hide things from the eyes of our all-seeing neighbors, companies, and public bodies? Or perhaps nobody, including pro-privacy advocates, is really convinced of the value of privacy? As far as the recognition of the importance of privacy is concerned, there seems to be no justification for pessimism. In spite of the prognosed lack of vitality, privacy presently leads a remarkably lively existence in newspaper opinion columns and in public debate.

Contribution received in 2010.

A. Vedder (✉)
TILT – Tilburg Institute for Law, Technology and Society,
Tilburg University, Tilburg, The Netherlands
e-mail: anton.vedder@tilburguniversity.edu

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*,
Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_2,

This public debate, however, deserves special attention because it suffers quite considerably from superficiality. Participants cling to a simplistic definition of privacy. At the same time they tend to label the normative impact of everything related to information and information technology, in terms of privacy. Because we are on the brink of a new informatization wave, this is the right moment to explore and, if need be, update the notion of privacy.

How does privacy exactly relate to new technical developments and changing social relationships? What are the human and social vulnerabilities, and the exact values to which privacy relates in light of these changes and developments? In order to keep the notion effective, it needs to undergo some maintenance and renovation work every now and then.

2.2 The Public Debate

In public, policymaking and politics, the recognition of privacy as a value seems to be losing quite a lot of ground (cf., Albrecht et al. 2003, p. 104; Vedder 2006). Policymakers and members of government tend to defend this trend referring to the alleged decline in the common citizen's appreciation of privacy (Projectgroep Forensische Opsporing Raad van Hoofdcommissarissen 2004). Research into citizen privacy perception, however, provide no concrete confirmation of such a decline (Perri 6 1998; Koops and Vedder 2001; Schildmeijer et al. 2005; Verhue 2007; Koffijberg et al. 2009). Nevertheless, nearly all of these investigations do make it clear that the 'ordinary' citizen or consumer has an enormous lack of insight concerning the technical possibilities, regarding the retention and processing of data about them.

In the past few years, in many European countries, the public debate about privacy has particularly focused on the impact on privacy, by all kinds of measures to combat terrorism and major crime. In addition, the discussion was fueled now and then by the introduction of new services and techniques by companies, like Google (search machines that profile searchers, photography of home environments). All in all, this resulted in a lively debate with contributions from various authors.

Authors who cherish privacy are generally very good at pointing out threats founded on a certain security measure or on an electronic service, or new technique. For example, they make it clear in which situation certain personal data can be leaked and where there are loopholes in security systems. In their further interpretation of the notion they heavily rely on the European and national legal approaches to the protection of personal data (Directive 95/46/EC on the Protection of Personal Data). Central to this approach is the primordial status of the definition of personal data in terms of data that can be traced back to an individual unambiguously.

Protection of these data is aimed for in different ways, but all of these are centered on the ideal of the individual as the most important discretionary

authority with regard to 'his' personal data. In principle, the individual has the right to control who may have access to his personal data and what may be collected, processed or saved. This right is obtained in the form of permission or agreement requirements, inspection requirements, duties to specify the purposes of data collection and various rules for the transparency of the storage and processing of data. It must for example, be clear who is responsible for a collection of data, who the processor is, what the security conditions are, etc. Protecting privacy is thus protecting personal data by protecting (and re-establishing) the individual to whom the data refer to as the unique locus of control over their whereabouts and processing.

While in the current debate, people are very good in pointing out where a specific privacy problem might occur in a technical sense, they are less proficient in explaining why or in what way these risks exactly have to be taken seriously. It is as if the normative point of the notion, the gist of it, has been lost out of sight. Perhaps it is also for this reason that the debate does not provide much insight into the considerations that have to play a role when a balance must be struck between privacy and conflicting values and interests (see also Muller et al. 2007). It should not come as a surprise then that critics often complain that privacy in political discussions generally acts as a theoretical debate killer.

2.3 The Meaning of Privacy as a State of Affairs

There is a sharp contrast between this somewhat meagre view of privacy arising from the public debate and the views of privacy in the academic discussions between legal theorists and ethicists in scientific journals. During the latter part of the previous century, it was fashionable to start theoretical contributions on privacy with mentioning the 'conceptual chaos' surrounding the term. Judge Biggs found in 1956 that a haystack after a hurricane was in better shape than the conceptual structure of privacy (Prosser 1960; Johnson 1989a, p. 157; Parent 1983, p. 341). With all respect to the complainers in the past and present, it should be noted that debate and controversies are somehow natural to even the most ordinary normative notions (Gallie 1955–1956). It would indicate mental impoverishment if a society like ours did not regularly speak strongly about the conceptual constructions which are part of the foundations of our type of society.

After further consideration, the supposed chaos surrounding privacy does not appear to be so bad. The majority of the differences in opinion concern state of affairs in reality to which the notion of privacy can refer on the one hand and the normative function or point of the notion on the other. A large part of these theoretical clashes concerning privacy again are more latent than manifest.

Generally, it is presumed that with regard to the state of affairs to which privacy can refer, it makes sense to distinguish a physical-spatial, relational, decisional, and informational dimension. The multidimensionality is often only mentioned to explain that privacy should not be understood as merely something spatial—as

something restricted to the body and the immediate home environment of an individual (see Nissenbaum 1998).

Over the years nearly all the aspects present in the meaning of the term when it was originally introduced by Warren and Brandeis (1890) have been retained. It was only at the end of the nineteenth century that the word 'privacy' came to be used explicitly as a moral and legal normative term. The normative roots of the modern privacy term appear to go back a lot further. J.S. Mill (1806–1873) argues for the protection of the domain of individual freedom against intrusions by governments, social institutions and other citizens. Mill describes this as the inner domain of consciousness, conviction, and feelings (Mill1974; cf., Schoeman 1992, pp. 24–36; Holmes 1995, pp. 17–18). Furthermore, the notions of freedom of will, moral independency, and self-determination that gradually crystallized during the Middle Ages and the Renaissance were important for the development of the modern idea of privacy. In addition, the famous article by Warren and Brandeis itself shows how old notions regarding ownership implicitly affected the term privacy. Finally, conventions and cultural traditions concerning dignity and a person's status seem to play an important role.

Warren and Brandeis define privacy as a right of individuals to be protected against the unsolicited distribution of information concerning their private life, particularly via publications. According to them, private life concerns emotions, sensory experiences, feelings, thoughts, dealings, and includes personal relationships, relations, writings and statements (Warren and Brandeis 1890, p. 195). Both authors highlight the right to privacy in connection with a statement made two years earlier by Thomas McIntyre Cooley (1824–1898, judge of the Supreme Court of Michigan) concerning the citizen's 'right to be let alone by government, however, without identifying this with the right to privacy (Blok 2002).

There is a steady increase in both the social and theoretical debates about privacy during the second half of the previous century. A focus on what could be called the decisional dimension of privacy stabilizes for a while at the beginning of the 1960 and 1970s. In a number of rulings dating from this period, the Constitutional Court of the United States decided to interpret privacy as a kind of right to self-determination, a right for the individual to decide in a number of private matters.[1] This interpretation protects the right to privacy particularly against state regulatory pressure. Subsequently, the discussion focuses on the question as to how much freedom individuals should be allowed concerning choices about their private life. In particular, this concerns decisions about an individual's sexual preference, the use of contraceptives, abortion, etc. This discussion reminds us of a famous debate in the 1960s between the British

[1] The sources of this kind of interpretation can be found in: *Griswold* v. *Connecticut*, 381 U.S. 479 (1965); *Loving* v. *Virginia*, 388 U.S. 1 (1967); *Eisenstadt* v. *Baird*, 405 U.S. 438 (1972); *Roe* v. *Wade*, 410 U.S. 367 (1973).

Philosophers Hart (1963) and Devlin (1965) with respect to the neutrality of the state in relation to a citizen's views of the good life. The controversy is tenacious between proponents and opponents of 'privacy protection' in these questions. During the 1990s these questions flared up again in controversies between liberals and communitarians.

In the European and American literature of the late 1960 and 1970s, the concept of privacy is also often connected with the notion of intimacy of personal relationships (Aubel 1968; Gerstein 1978; Weinstein 1971). Many authors argue that family life must be immune from the judgement and interference by others. In these definitions, privacy is a sanctuary for intimate feelings. Feminist oriented legal professionals and ethicists questioned this argument (Allen 1988). During the 1990s, Inness defended the view that the intimacy of dealings, choices, and information should determine whether these should be considered to be worthy of protection. She provides an exhaustive, strongly normative elaboration of the term 'intimacy' (Inness 1992, pp. 10, 74–94).

Starting from the mid-1960s we also observe an approach to the concept in which privacy is almost completely defined in terms of the information about people (Westin 1967; Henkin 1974; Rule 1980; Parent 1983; Lyon 1994; Powers 1996; Etzioni 1999). The enormous flourish of mass media and the cautious emergence of new types of communication and techniques for data processing (the introduction of personal computers) undoubtedly gave rise to this. The idea of informational privacy is the basis of the previously mentioned European directive and national legislation regarding the protection of personal data. This approach to the idea particularly tends to be interpreted in terms of access to information about individuals. Even physical and spatial access is sometimes interpreted in terms of information (for example but not uniquely: Johnson 2001).

In all the more or less latent controversies about the priority of one of the dimensions, other points of view play a role as well. The role of social and cultural conventions and traditions regarding the meaning of privacy is sometimes highlighted (Stein and Shand 1974; Moore 1984; Johnson 1989a, b); Barth et al. 2006). This part of the discussion makes clear that the term privacy is not a rigid theoretical construction but also accommodates strong culturally dependent norms. I will come back to this point later on.

Another part of the discussion concerns the question whether privacy is a form of isolation as such or a form of controlled isolation. Unquestionably, from the beginning of the 1970s onward, privacy is being defined as spatial, relational or informational accessibility controlled by the individual (Westin 1967; Parent 1983). For example, Fried (1968, p. 209) defines privacy as, 'the control we have over information about ourselves.' Another author, Rachels (1975a, b, p. 326) talks of 'the ability to control who has access to us.' This line of discussion makes it very clear that contact with the outside world does not necessarily have to be uncomfortable with privacy when the individual remains in control of who has what kind of access to him.

2.4 The Meaning of Privacy as a Value

Does privacy present a value in itself, or is it of mere instrumental importance or a constituent, i.e., a representing part of another value? Which values are precisely at stake when infringements of privacy are observed?

There are hardly any scholars who are prepared to defend privacy as being intrinsically valuable. The only one who comes close to doing this is Benn (1988). His ideas about the relationship between privacy, autonomy, and dignity, can however be better defined in terms of constituent values: in his view, respect for personal privacy is derived from respect for the autonomy and the dignity of individuals (also cf., Bloustein 1964). The same is true for authors who—continuing along the lines of the discussions during the 1960 and 1970s concerning the decisional dimension—particularly connect privacy with individual freedom (Johnson 1989b; Gutwirth 1998; Rössler 2001). Others seem to see privacy more as being instrumentally valuable to material interests, like being able to get a job or insurance, having the right to emotional and physical tranquillity and to protection against defamation or loss of status (Rachels 1975a, b, pp. 323–333; Johnson 1994, pp. 81–102). In addition, social interests like facilitating relations and social links are often named as part of the normative view on privacy (Rachels 1975a, b; Schoeman 1984, 1992). Finally, some authors advocate the idea inspired by Mill (1974) and Foucault (1975) that privacy can be advantageous for the diversity of ideas and creativity in society. From this point of view, privacy provides a sanctuary against the disciplinary effect of mass opinion and the demands of a controlling government or the tyranny of big companies.

All the variations in focus and different views that I have briefly described above should not be understood as different or even consecutive stages in a linear historical process since the introduction of the term by Warren and Brandeis. When a new interpretation of the term is introduced, old definitions do not just disappear. Since the 1950s of the last century, there is a reasonably orderly situation. Hiding behind the refined theoretical controversies there is a useable broad privacy notion based on the relative inaccessibility to individuals by other parties. This inaccessibility can be spatial inaccessibility or refer to the relative absence of observation by instruments or of representation in data and information. It is surprising how much of Warren and Brandeis' original notion has been kept alive. In the theoretical debate, monistic views about the value of privacy also seem to be put aside for notions about privacy as polyvalent: privacy as a servant to different values (cf., Thomson 1975a, b; Vedder 1996, 2000).

The differences in focus and the appearance of various definitions can be in good part explained by the need to protect individuals against the risks that come along with people's vulnerabilities that are transforming as a result of technical and technological developments, changes in the socio–economic relations, disappearing lines of demarcation between the private and the public sector, and altering conventions and traditions (Vedder 1996). Previously, I briefly suggested that the rise of mass media and the introduction of the personal computer have influenced

the understanding of privacy in terms of access to data and information concerning individuals. Something similar seems to occur regarding conventions and traditions. These factors can cause a certain vulnerability to which privacy norms can provide a protection barrier (Vedder 2000). Conventions and taboos concerning the (naked) body, the practice of certain biological functions (e.g., sex), talking with and about intimate relations etc., make people vulnerable in terms of loss of status and reputation if they are seen, observed or tape recorded. Privacy norms provide protection against these risks of loss of status and reputation by having these activities generally conducted in seclusion and by ensuring that this seclusion is respected. At the same time, where the purpose of these conventions is no longer clear or experienced, the question is what is really more effective: applying privacy norms or changing the taboo? (Sometimes the conventions or taboos seem to disappear by themselves. The rise of the mobile telephone seems in any case to have gone hand in hand with a reduction of the restrictive conventions and taboos about speaking with and about intimate relations. The call for protection through privacy norms does not seem to be so strongly needed any longer.)

2.5 Normative Impact of Ambient Intelligence and Converging Technologies

The social debate on privacy would benefit from input from the theoretical controversies. The popular and superficial notion of privacy in the public debate is, for instance, unsuccessful in uncovering the relevant risks for citizens involved in all kinds of technology-related measures against crime and terrorism. The consequences of group profiling, for example, cannot be well articulated with the help of this privacy concept because of the inherent restriction to personal data in the strict sense. There is also a need to pay attention to other normative principles like those of equality and fairness (Vedder 1997, 1998, 2006).

In two recent critical studies (Winter et al. 2008; Brouwer et al. 2009) concerning the Dutch Personal Data Protection Act ('Wet bescherming Persoonsgegevens') and its enforcement, far reaching changes were called for. Unfortunately little attention was given to the radical consequences of some imminent technical developments for the basic principles of the act.

Two developments in technology will drastically change our world in the coming 10–15 years: ambient intelligence and converging technologies. Ambient intelligence refers to the gradual integration of technical devices and technology in the environment and leads to more and better communication between devices and their users. This is possible because of three movements:

- Advanced miniaturization of computers, sensors and actuators (small instruments that start these processes or adjust them);
- Increase in storage, transmission, and processing capacity of data; and
- Omnipresence of networks and wireless communication possibilities.

Devices will be less dependent on manual operation through buttons, menus or keyboards and screens. They will be able to determine what we expect from them and, consequently, react or anticipate this. They will also be able to communicate more and better with each other, which means that the functionality of the used techniques and applications will increase enormously.

Converging technologies refer to the cross-pollination between nano technologies, biotechnologies, information and communication technologies, and cognitive science. The fusion of some or all of these technologies create new possibilities to externally intervene in people's behavior and can serve as a substitution for the present ways of influencing people, such as upbringing, education, pills, fences, walls and, written and unwritten rules/laws (Teeuw and Vedder 2008); Vedder 2008a, b).

What impact will these technologies have on our normative standards? To start with they will make it necessary to earnestly adapt the laws and rules concerning privacy and data protection. With the event of ambient intelligence and converging technologies, more information must be generated, processed, and combined than we can presently imagine. In order for these technologies to work, all kinds of information about individuals will continuously be collected and analyzed, concerning their physical condition, location, and context (for example, family and social background). These developments make the conceptualization of privacy as we know it from the social debate and the European and national legislation largely obsolete. Firstly, the assumption that individuals should be in a position to control what happens to the data and information about them cannot be maintained in this future scenario. The system of information flows will simply become too complex and incomprehensible. Secondly, the present notion is restricted to personal data which are very rigidly defined as data that can be traced to individuals. The great amount of data and information generated in the future will not be about personal data but about profiles of groups, that can often not be traced back to individual persons in the way that currently personal data is defined.

Finally, there will be important consequences for which the present privacy-approach does not provide us with any tools for direction. The use of converging technologies will lead to an increase in data about people's physical and clinical status. In fact this will result in an enormous expansion of the domain of medical data. Medical data will no longer merely be relevant in traditional health care and insurance domains, but expand to the domains of security and education. As ambient intelligence and converging technologies will play a bigger role in areas like security and education, they will lead to unprecedented medicalization. Physical and biological data about persons will be needed to make these applications work. These data may however indirectly reveal important information about the medical condition of the persons involved, in the same way as iris scans used for border crossing procedures may reveal information about illnesses of the passengers whose irises are scanned already now. This new medicalization and, more in general, the further expansion of information flows in our society will require radical reconsideration of the current privacy approach.

Again, reconceptualizaton of privacy is in itself not sufficient to come to terms with the normative impact of ambient intelligence and converging technologies. We should also be aware of other consequences. In 10–15 years' time, for reasons of efficiency and effectivity, the state will allow traditional regulatory enforcement to be carried out by automated means. This is already happening on a small scale by means of relatively simple technologies, like roundabouts and speed bumps used in traffic control. In the future, people's behavior can be influenced in a much more sophisticated way by instruments that either directly affect them or make changes to their environment which in turn will change their behavior. Private parties will be contracted for the production, management, and maintenance of these techniques. As a result of large scale availability and ultimately lower investments, the use of ambient intelligence applications and converging technologies for 'private regulation' will also increase in the coming ten years. Both the delegation of traditional state regulation and enforcement to private parties as well as private regulation arrangements create new demarcations of the public and the private, and call for reflection on the controllability and legitimacy of these new regulation and enforcement schemes.

There is another point of concern. Given, that it is highly attractive to incorporate regulation for reasons of efficiency and effectivity in technical devices, the temptation to merge the rules of technique with those of enforcement will increase. In traditional forms of regulation, such as law and social morality, it is possible to make a distinction between knowing a norm and deciding whether to act accordingly. When making this decision, there is a certain freedom because you can choose not to abide by the rule in spite of the risk of sanctions. When the norm and enforcement are merged through technical devices, people will automatically be forced to follow the rule: they will stop for a red light not because they want to but because they have no other choice. Technology will make them stop. This is interesting for two reasons. Firstly, it must be ensured that the right rules are incorporated in the technical devices and that they are applied fairly and reasonably. Justified civil disobedience is difficult or impossible. Secondly, knowledge of norms and moral motivation to follow norms (e.g., because you consider the norms good or because you want to be a good person) become needless. However, in many ideologies and philosophical-ethical streams, autonomous moral motivation is considered very important, in itself and because without the autonomous moral motivation individuals become morally lazy; the sensitivity and principal willingness to act according to norms may become redundant which could have a severe impact if these technical devices would fail to work at a certain moment.

2.6 Conclusion

In view of present and future technological developments, a more in-depth social debate about privacy enriched with elements from the ethical and legal theoretical debate, is important. Privacy is not a simple and elegant term as the present social

debate might insinuate. Privacy is a complex term and must be substantiated with the help of insights from the theoretical debate. The analytical potential of the popular notion of privacy is limited. To do justice to the real problems and risks of new technologies, privacy should be viewed as a notion that plays an instrumental role in protecting individuals, not merely in light of their naturally human vulnerabilities, but also from the viewpoint of constantly changing circumstances in the socio–economic relationships, the boundaries between the private and the public sector, and conventions and traditions. The underlying values at stake are autonomy, welfare, equality, justice, dignity, status, and tranquillity. By pinpointing the values at stake and explaining precisely when there is a breach of privacy, we clarify the importance and the meaning of the breach.

Naturally, it will not always suffice to give a fully well reasoned assessment in the event a normative conflict with other values or interests arises. The precise meaning of a breach of privacy is often not easy to illustrate in terms of concrete detrimental effects for, for example, the welfare or the freedom of the individual in question. This applies even more to the ideals of diversity and creativity in a society inspired by Mill and Foucault. The disciplining or normalizing effects of observation and surveillance systems (adaptation of own behavior, not to be conspicuous for fear of being observed) can, in principle, be seen as a threat for diversity and creativity. Nevertheless, it is difficult to determine when observation would instigate behavior adaptation or how these possible adaptations should be qualified exactly. If observation or surveillance systems do lead to changed behavior and lifestyle, a good reason should be given to accept this disciplining effect.

Finally, privacy is important but not all-important. On the one hand, sometimes the benefits and advantageous opportunities offered by new technological applications simply outweigh the privacy risks. On the other, technological applications may have other important drawbacks, which are easily overlooked when privacy is considered to be primordial.

References

Albrecht HJ, Dorsch C, Krüpe C (2003) Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation. Freiburg, Max-Planck-Institut. http://www.iuscrim.mpg.de/verlag/online/Band_115.pdf

Allen AL (1988) Uneasy access: privacy for women in a free society. Rowan & Littlefield, Totowa

Aubel CP (1968) Persoon en Pers (diss. Nijmegen KUN). Deventer, Kluwer

Barth A et al (2006) Privacy and contextual integrity: framework and applications. Proceedings of the IEEE symposium on security and privacy, May 2006 (Showcased in 'The Logic of Privacy' The Economist, 4 January 2007)

Benn SI (1988) A theory of freedom. Cambridge University Press, Cambridge

Blok PH (2002) Het recht op privacy. De betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht (diss. Tilburg). Boom Juridische Uitgevers, Den Haag

Bloustein EJ (1964) Privacy as an aspect of human dignity. An answer to dean Prosser. New York University Law Review, pp 962–1007. Also in: Schoeman FD (ed) (1984) Philosophical dimensions of privacy: an anthology. Cambridge, Cambridge University Press, pp 156–202
Brouwer A de et al (2009) Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer. Ministry of Interior Affairs, The Hague
Devlin P (1965) The Enforcement of Morals (1st edn. 1959). Oxford University Press, Oxford
Etzioni A (1999) The limits of privacy. Basic Books, New York
Foucault M (1975) Surveiller et punir, naissance de la prison. Gallimard, Paris
Fried C (1968) Privacy. Yale Law J 77:475–493
Gallie WB (1955–1956) Essentially contested concepts. Proceedings of the Aristotelian society, pp 167–198
Gerstein RS (1978) Intimacy and privacy. Ethics, pp 76–81
Gutwirth S (1998) Privacyvrijheid! De vrijheid om zichzelf te zijn. Rathenau Instituut, Den Haag
Hart HLA (1963) Law, liberty and morality. Oxford University Press, London
Henkin L (1974) Privacy and autonomy. Columbia Law Rev 74:1410–1433
Holmes R (1995) Privacy: philosophical foundations and moral dilemma's. In: Ippel P (ed) Privacy disputed. SDU Uitgeverij, Den Haag, pp 15–27
Inness J (1992) Privacy, intimacy and isolation. Oxford University Press, Oxford
Johnson JL (1989a) Privacy and the judgements of others. J Value Inq 23:157–168
Johnson JL (1989b) Privacy, liberty and integrity. Public Aff Q 3:15–34
Johnson D (1994) Computers and privacy. Prentice Hall, Upper Saddle River
Johnson JL (2001) Immunity from the illegitimate focused attention of others: an explanation of our thinking and talking about privacy. In: Vedder A (ed) Ethics and the internet. Antwerpen, Intersentia
Koffijberg J et al (2009) Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving. Den Haag/Amsterdam, College Bescherming Persoonsgegevens/Regioplan
Koops BJ, Vedder A (2001) Opsporing versus privacy: de beleving van burgers. SDU Uitgeverij, Den Haag
Lyon D (1994) The electronic eye, the rise of the surveillance society. Polity Press, Cambridge
Mill JS (1974) On liberty (1st edn. 1859). Pelican Books, London
Moore B (1984) Privacy: studies in social and cultural history. M.E. Sharpe Inc. New York
Muller ER, Kummeling HRBM, Bron RP (2007) Veiligheid en privacy, Een zoektocht naar een nieuwe balans. Boom Juridische Uitgevers, Den Haag
Nissenbaum H (1998) Protecting privacy in an information age: the problem of privacy in public. Law Contemp Probl 17:559–596
Parent WA (1983) Recent work on the concept of privacy. Am Philos Q 20(4):341–355
Perri 6 (1998) The future of privacy. Demos, London
Powers M (1996) A cognitive access definition of privacy. Law Philos 15:369–386
Projectgroep Forensische Opsporing Raad van Hoofdcommissarissen (2004) Spelverdeler in de opsporing. Een visie op forensische opsporin (z.p.). http://www.politie.nl/Overige/Images/33_144778.pdf
Prosser WL (1960) Privacy. Calif Law Rev 48:338–423
Rachels J (1975) Why privacy is important. Philosophy and public affairs, pp 323–333
Rachels J (1975) Why privacy is important. In: Schoeman FD (ed) (1984) Philosophical dimensions of privacy: an anthology. Cambridge University Press, Cambridge, pp 290–299
Rössler B (2001) Der wert des privaten. Frankfurt am Main, Suhrkamp
Rule J (1980) The politics of privacy: planning for personal data systems as powerful technologies. Elsevier, New York
Schildmeijer R, Samson C, Koot H (2005) Burgers en hun privacy, Opinie onder burgers. Amsterdam, TNS/NIPO
Schoeman FD (1984) Philosophical dimensions of the literature. In: Schoeman FD (ed) Philosophical dimensions of privacy: an anthology. Cambridge University Press, Cambridge, pp 1–33

Schoeman FD (1992) Privacy and social freedom. Cambridge University Press, Cambridge
Stein P, Shand J (1974) Legal values in western society. Edinburgh University Press, Edinburgh
Teeuw WB, Vedder AH (eds) (2008) Security applications for converging technologies, Impact on the constitutional state and the legal order. Boom Juridische Uitgevers, Den Haag
Thomson JJ (1975a) The right to privacy. philosophy and public affairs, pp 295–315
Thomson JJ (1975b) The right to privacy. In: Schoeman FD (ed) (1984) Philosophical dimensions of privacy: an anthology. Cambridge University Press, Cambridge, pp 272–289
Vedder A (1996) Privacy en woorden die tekort schieten. In: Nouwt J, Voermans W (eds) Privacy in het informatietijdperk. SDU Uitgeverij, Den Haag, pp 17–30
Vedder A (1997) Privatization, information technology and privacy: reconsidering the social responsibilities of private organizations. In: Moore G (ed) Business ethics: principles and practice. Business Education Publishers Ltd, Sunderland, pp 215–226
Vedder A (1998) Het einde van de individualiteit? Groepsprofilering, datamining en de vermeerdering van brute pech en dom geluk. Privacy en Informatie 1(3):115–120
Vedder A (2000) Medical data, new information technologies and the need for normative principles other than privacy rules. In: Freeman and Lewis (ed) Law and medicine (Series Current Legal Issues) Oxford University Press, Oxford, pp 441–459
Vedder A (2006) Niets meer te verbergen en toch nog bang. Filosofie en Praktijk 27(5):47–61
Vedder A (2008a) Convergerende technologieën, verschuivende verantwoordelijkheden. Justitiële Verkenningen 34(1):54–66
Vedder A (2008b) De oudere en de paradoxale gevolgen van nieuwe technologieën. In: Berg M Van den, Prins JEJ and Ham M (ed) In de greep van de technologie—Nieuwe toepassingen en het gedrag van de burger. Van Gennep, Amsterdam, pp 135–150
Verhue D (2007) Nationaal Vrijheidsonderzoek—opiniedeel. Meting 2007. Amsterdam, Veldkamp/Comité 4 and 5 May 2007. http://www.4en5mei.nl/mmbase/attachments/110429/2007.04.284_Veldkamp_Marktonderzoek_BV_Nationaal_Vrijheidsonderzoek_2007_opinie
Warren SD, Brandeis LD (1890) The right to privacy. The implicit made explicit. Harv Law Rev, pp 193–220. Also in: Schoeman FD (ed) (1984) Philosophical dimensions of privacy: an anthology. Cambridge University Press, Cambridge, pp 75–103
Weinstein WL (1971) The private and the free: a conceptual inquiry. In: Pennock JR, Chapman JW (eds) Nomos XIII: privacy. Atherton Press, New York, pp 88–104
Westin A (1967) Privacy and freedom. The Bodley Head, New York
Winter HB et al (2008) Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de wet bescherming persoonsgegevens in de praktijk. WODC/Ministerie van Justitie, Den Haag

Chapter 3
Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications

Irma van der Ploeg

Abbreviations

ICAO International Civil Aviation Organization
MRTD Machine Readable Travel Documents

Contents

3.1 Introduction 29
3.2 Human Differences and the Biometric Body 30
3.3 Sensitive Categories, "Partial Identities" and Soft Biometrics 33
3.4 A Transparent and Unobtrusive Future? 36
3.5 Conclusion: Critiquing Normativities in the Informatization of the Body 38
References 38

3.1 Introduction

Whereas biometrics is generally conceived of as using certain features of "the" human body for IT-mediated authentication and identification, we are all aware that "the" human body does not exist. People come in a variety of shapes, colors, genders, and ages, sharing, of course, most of their physiology and anatomy with

Contribution received in 2010.

I. van der Ploeg (✉)
Infonomics and New Media at Zuyd University, Maastricht, The Netherlands
e-mail: i.vdploeg@hszuyd.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_3,

most of humanity, but never all. Moreover, these differences between people are commonly used to categorize people in ways that are of great ethical, legal, and political significance (Foucault 1975; Lacqueur 1990; Duden 1991; Schiebinger 1993). There are at least two different ways in which issues of human bodily differences emerge in relation to biometric technologies.

On one hand, there is a matter of exclusion of certain categories of "different" people from system use, because the systems can only cope with difference to a limited extent. In biometric discourse the set of problems connected with this issue is referred to with a number of concepts, such as, for example, "usability," "accessibility," "failure to enroll," "exception handling", and "template aging." In the discourses of social theory and politics, these matters invoke considerations in terms of distinctions made between normal and abnormal or rule and exception. Such notions, then, are connected with concepts like "normalization" and social inclusion and exclusion (Foucault 1977, 1979; Star 1991). "Normalization" here refers to the production and enactment of norms, through which the very distinction between what counts as normal and what as exception or deviancy is performed within and through technological practices. When a biometric system fails to cope with variations in human features falling outside a certain range, it thereby categorizes and excludes, with more or less serious consequences to the people concerned.

On the other hand, the issue of bodily differences emerges with systems that use the differences mentioned, trying to automatically classify people in gender, age, ethnic, height, or weight categories. So-called "soft biometrics," a set of experimental biometric applications aiming at recognizing general body characteristics uses what, within technical discourse, are referred to as "partial identities." Here, questions about the black-boxing of contingent, perhaps unscientific and contestable, or even unethical constructions of those categories, by building them into the systems, may arise (Latour 1987; Bowker and Star 1999).

This chapter sets out to question the normative assumptions about human bodies embedded in biometric technologies, and to articulate and discuss issues emerging from the various ways in which biometric technologies and human bodily differences interact and interfere with each other. It will do so in particular in relation to 'next generation biometrics' such as soft biometrics, physiological biometrics, and distant sensing technologies.

3.2 Human Differences and the Biometric Body

Underlying the very idea of biometric technologies as automated identification and authentication tools is a conception of the body that is rather paradoxical. On one hand, biometrics is based on the biological fact that every individual is physically unique. No two fingerprints are identical, everybody's irises are different from those of an other, the same way that no two faces, voices, or retinas are exactly the

same. This is the condition of possibility of the very idea of biometric technologies as identification tools.

On the other hand, however, there is a simultaneous assumption of similarity: every human person is assumed to have a clearly audible voice, a set of ten fingerprints, two irises, and a recognizable face, and so on. Though hardly ever mentioned as such, this assumption of similarity is as crucial to the functioning of biometric systems as is the assumption of uniqueness. With respect to the human bodily features used in biometrics, this means that there is an assumption of normality that is defined as a range of variations that constitute "the normal." Such notions of normality are built into the equipment: hand scanners have particular shapes, with designated places to put the fingers; fingerprint systems are designed for the registration and comparison of a particular number of fingerprints, cameras to scan faces are directed at a specific height, and the accompanying face recognition software often works best for a particular shade range of skin color, and so on.

Next to the assumptions about unicity and similarity, there is an additional assumption regarding the stability of the body over time. Although the physical features used for biometric identification purposes are chosen precisely because they are relatively stable and universal, the operative word here is "relatively." Like all living matter, human bodies change over time. Besides the natural processes of development and aging, bodies wear the signs of their histories: scarring and other damage, facial signs of hardship and worries, prosthetic additions to compensate functional losses are all part and parcel of living and interacting with the world during a lifetime. Manual labor may wear down fingerprints that only became "machine readable" from somewhere around the age of 12 in the first place; disease may alter eyes, the same as surgery or sorrow can change faces.

For many purposes the assumptions mentioned may be quite reasonable, but when it comes to the large-scale applications we see implemented today, such as, for instance, Eurodac, VIS, US-VISIT, SIS-II, and the e-Passport, the implied notions of similarity and stability quickly prove to be what they are: abstractions that may fit a majority, but actually exclude significant numbers of people.

While it is true that most technology has an "in-built" more or less narrowly defined standard "user," this is not always problematic (Woolgar 1991; Akrich 1992). Products may be designed for specific groups rather than a mass market, and also, in consumer technological products, the need to seduce people to buy and use makes for the best possible incentive to cater to individual tastes, possibilities, and desires. The above-mentioned, extremely large-scale systems, however, are often obligatory for people to exercise some right, or procure a service, such as free movement and travel, collecting benefits, or applying for asylum (van der Ploeg 1999a, b; Brouwer 2007). Hence, these systems are not catering to the needs or desires of individuals, but instead are built to "process" (sometimes extremely) high numbers of people as fast as possible. The priority of 'high through-put' in today's border management makes for a highly standardized technology, where increasing flexibility quickly leads to losses in speed, accuracy, and effectivity. To the extent that the assumptions of similarity and stability built into the systems are unwarranted, large-scale applications can, therefore, be expected to run into

difficulties. And so, according to most experts, they will (Koslowski 2005). In the context of biometric technologies, "accessibility" refers to the problem that many people, often specific categories of people like the elderly, children, people from particular ethnic or professional backgrounds, are unable to enroll in a biometric system because they do not possess the required bodily feature or a sufficiently "machine-readable" one.

Almost all biometric techniques present, for instance, an age range in which the biometric data can be optimally acquired and processed. In the very young, the height of the papillary relief is still underdeveloped, whereas in the elderly it often shows a "wearing down." Most research attention has gone to the upper age limit and the problem of 'template aging,' defined as the degree to which biometric data evolve and change over time, and the extent to which templates fail to account for this change. Little research has been done on minors and children, with the study by Den Hartog and colleagues 2005 being an exception. One of the major conclusions in this study involving some 160 toddlers concerned not merely the often un-machine-readability of their fingerprints, but also the difficulty of getting the small ones to "cooperate" sufficiently. Acquiring good quality fingerprints, or even facial photographs for that matter, requires a level of understanding and cooperation, a willingness to present the hand (not a clammy, clenched little fist) for processing, to sit still, to not cry and wriggle about, and, for today's passports' facial photographs, not laugh or smile—exigencies that turn out to be near impossible to demand from the very young. "You really have to like children" was one of the side comments of one of the researchers in the study.

This point, however, also suggests a third assumption about bodies that most biometric systems embody to a certain extent, and in a variety of ways. This one has less to do with the body as a physical object, but rather with the body as the "site" of culturally and emotionally encoded embodied experience, and the way it is enrolled in biometric technological configurations (Haraway 1991; Bordo 1993; Hayles 1999; Merleau-Ponty (1945) 1962). Biometric systems generally presuppose the availability of the body for handling in certain ways, scanning and assessing it, as a prerequisite for the system to work. In Actor Network Theory's terms, it is enrolled in a quite particular way. In some cases this implies a visibility, in others touchability, and generally one can see here a demand for it to take certain postures, perform certain gestures, and allow or enable it to be processed in a number of ways. The requirements for ICAO compliant facial photographs for machine readable travel documents (MRTDs), for example, show a detailed list of prescriptions concerning posture, expression, what not to wear, and how to pull hair back to present ears (Home Office Identity and Passport Service). In the case of the toddlers it is easy to imagine how the requirements concerning the disciplined and docile availability of hands and faces is an unrealistic expectation that can become the cause of genuine distress, if, for example, an enrollment procedure in an unfamiliar environment, performed by a uniformed officer has to be repeated several times to acquire "usable data".

However one can also imagine the feelings of anxiety, or humiliation and anger that compliance with the demands of the systems may instill, in, for instance,

people deeply bound to certain cultural or religious norms of modesty and privacy, who are asked to remove veils in a public space, stick out their hands to be touched by a stranger. Comparable to the problems the export of western medicine to other cultures was confronted with because of its ways of examining bodies, or the distress caused in some indigenous peoples by photography, there is a sense in which biometrics similarly imposes a certain cultural norm concerning the availability and usability of bodies on people who may not share these norms.

The specific form in which the assumptions of similarity, stability, and availability are materialized in a particular biometric system determine who is and who will not be excluded from enrolling in it, who will and will not experience difficulties using it. As access to more and more services and entitlements is regulated by biometric identification, the fact that certain people will be systematically excluded or otherwise disadvantaged becomes a problem with socio-political and ethical implications.

And, even though many efforts are directed today at extending the range of variety a system can cope with, for example by improving the image resolution of the scanners, imperfections of the systems are often downplayed. However, even the smallest percentage of "non-machine readable" people will amount to unacceptably high numbers when a system is rolled out on a large scale. Moreover, the very fact of being required, but physically or otherwise unable to comply with the demands of a system said to be "for everyone," and maybe even being asked for explanations, can in some situations be experienced as awkward or painful. But above all, if the in-built normative assumptions remain unacknowledged to the extent they are today, responsibility for remedying the situation for those excluded or disadvantaged by the systems is less likely to be taken up adequately.

3.3 Sensitive Categories, "Partial Identities" and Soft Biometrics

In 1998, Wayman, then director of the National Biometric Test Centre at San Jose State University, testified in a US congressional hearing:

> We must note that with almost all biometric devices, there is virtual no personal information contained therein. From my fingerprint, you cannot tell my gender; you cannot tell my height; my age, or my weight. There is far less personal information exposed by giving you my fingerprint than by showing you my driver's license (Castle 1998).

Despite such reassurances, the at that time still relatively unknown biometric technologies had some people worried enough to insist that: "collection of a biometric identifier must not conflict with race, gender, or other anti-discrimination laws" such as, for example, in the proposals for the Californian Consumer Biometric Privacy Act (Mintie 1998).

Although this was then seen by many biometrics advocates as being based on unfounded and ill-informed beliefs about biometrics, historian Simon Cole writes the following on the presumed "emptiness" of fingerprints:

> Galton's [the founder of dactyloscopy] "regret," his failure to find the key to the code of heredity in fingerprint patterns, has been confused with the notion that fingerprint patterns actually contain no information pertinent to health, ancestry or behavior. But other researchers found rough correlations between fingerprint pattern type and ethnicity, heredity and even some health factors. These correlations, especially the ethnic ones, have proven robust and still hold up today. As with any correlation, they are not determinative; one cannot predict ethnicity from fingerprint pattern, but fingerprint pattern types do appear with different frequencies among different "ethnic groups" (as defined by researchers) … In short, the perceived "emptiness" and harmlessness of fingerprint patterns is a social achievement, not a natural fact (Cole 2006).

Moreover, a few years after the congressional hearing, it has become more evident that Wayman may not have been entirely right: in an article on so-called 'soft biometrics,' we read:

> *Many existing biometric systems collect ancillary information like gender, age, height, and eye color from the users during enrollment.* However, only the primary biometric identifier (fingerprint, face, hand-geometry, etc.) is used for recognition and the ancillary information is rarely utilized. We propose the utilization of "soft" biometric traits like gender, height, weight, age, and ethnicity to complement the identity information provided by the primary biometric identifiers (Jain et al. 2004, emphasis added, IvdP).

In my view, today's developments in "soft" biometrics, i.e., a set of experimental biometric applications aiming at using "partial identities,"and recognizing general body characteristics such as body weight, gender, age, or ethnicity, signifies a new step in the informatization of the body that needs critical attention urgently (van der Ploeg 1999a, b, 2003, 2008). After all, the targeted characteristics concern highly sensitive categories, many of which are over-burdened with histories of discrimination of the worst kind.

In this context, however, they are called "soft," because unlike biometric identification technologies, they focus on traits that do not single out one individual from all others, but on ones that are shared by large numbers of people. From an identification perspective, however, that can be useful as supporting information or "secondary mechanism," which, when used in conjunction with identifying biometric traits, can substantially improve the success rates of identification technologies. In addition, they can be used to establish membership of a category (e.g., establishing adulthood) without actually identifying, for which reason a certain privacy–protective potential is sometimes attributed to these technologies (Li et al. 2009). Beyond this, however, the quoted article gives a few lines of research, which clearly point to more far-reaching potential applications:

> The effectiveness of utilizing the soft biometric information for "indexing" and "filtering" of large biometric databases must be studied. Finally, more accurate mechanisms must be developed for automatic extraction of soft biometric traits (Jain and Lu 2004).

One could imagine useful applications of systems that can categorize, e.g., faces, according to gender or ethnicity, or "filter" a database that way, for example when a reliable witness statement in a crime investigation would enable exclusion of particular categories from a police database search. Another such example would be classifying subjects in broad age categories, in order to determine legal competence to apply for certain services, or buy certain products, while preserving anonymity. The potential to provide a broad categorical classification rather than full identification is often invoked as a privacy enhancing quality soft biometrics may provide (Li et al. 2009). On the other hand, there are all too many situations imaginable in which filtering people out on the basis of their gender, age, or ethnic/racial background constitutes illegal discrimination, and developing systems to automate this process could, therefore, be considered inherently risky (Lyon 2003).

Also, and contrary to what their apparent self-evident reference in ordinary language and everyday life may lead one to believe, the reification of these categories and distinctions, as the history and philosophy of science have made abundantly clear, is essentially contestable and unstable (Lacqueur 1990; Schiebinger 1993). For example, the distinction between the male and female gender on a genetic level does not always match the one made on an endocrinological, anatomical, psychological, or socio-cultural level; and even when birth registered gender is taken as a reference point, a problem exists where this is amenable to change during an individual's lifetime. In an exacerbated form, similar problems exist with ethnicity and race classifications, all of which have been proven to lack any indisputable basis in "nature" (Harding 1993; Fausto-Sterling 2008).

A telling example of the way such important insights will be ignored in soft biometrics is the research by Jain and Lu (2004) into the development of a system for ethnic classification. In this study facial images from two separate databases, pre-defined as the "Asian database" and the "non-Asian database," were divided into a training set and a test-set. From that original, previously categorized training set, the system was to learn, and be able to continue classification of subsequently fed test images. Performance of the system subsequently was evaluated (percentage of "correct" classifications) by the researchers again. On the issue of which definition of "ethnicity" to use, and what criteria to apply, the authors state:

> In this paper, we do not make a distinction between the terms "ethnicity" and "race," which are used to refer to people who share *common facial features that perceptually distinguish them* from members of other ethnic groups (Jain and Lu 2004, p. 1, emphasis added IvdP; please note the circularity of this definition).

and:

> Because the robust facial landmarks localization is still an open problem due to the *complex facial appearance in the real-world environment* … we explore the appearance-based scheme, which has demonstrated its power in facial identity recognition (Jain and Lu 2004, p. 2, emphasis added, IvdP).

In other words, in order to render the great human diversity in "the real world environment" technologically manageable in "laboratory conditions," recourse is

taken to a method based on appearances, on top of which, for the purposes of this study:

> The task is formulated as a two-category classification problem, to classify the subject as an Asian or non-Asian (Jain and Lu 2004, p. 2).

Following the insights developed in Actor-Network theory-based studies into the way laboratory developed technologies are made to "work" outside the laboratory (e.g., Latour 1983), there is a good reason to worry about what such systems will require to happen with ethnic and racial categorizations in "the real world" when people decide this needs to be made to work. What emerged from these studies is, one may remember, how "real world" practices are adapted and transformed, to copy the conditions under which technologies worked in "the laboratory," in order to repeat functionality and successful performance elsewhere. This might mean that, for all practical purposes, and in as of yet unknown situations, we may come to adapt our thinking about human diversity to fit the inbuilt categorizations and definitions of the systems.

Whereas the literature on the history of the categories of sex and gender, ethnicity, and race has provided us with ample proof of their deeply problematic nature, this literature had the advantage of having scientists' texts, language, observable practices, and visual representations as its relatively accessible objects of study. The development toward "soft biometrics", however, implies that whatever definitions of the categories in question are going to be used, they will become inscribed in software and algorithms far more difficult to assess, and therefore, to contest. This fact renders this technology fraught with risks of various kinds, risks that will undoubtedly increase when these systems are applied in an embedded and "unobtrusive" fashion.

3.4 A Transparent and Unobtrusive Future?

So far several issues concerning biometrics and bodily differences have been discussed, focussing on the several ways in which normative assumptions and dimensions of difference and sameness are built into the systems. These assumptions concern the similarity and stability of human bodies and their features, in addition to which a third assumption concerning a presumed docile availability was described.

In relation to the latter, a significant development is worth noting, namely the number and extent of efforts we see emerging today to develop biometric systems that do not need the active cooperation of people anymore. Biometric sensing from a distance is high on the R&D agenda today, enabling the design of systems that can be applied without people even being aware that they are being identified, registered, or assessed. For example, Li et al. (2009) describe how the NSTC Subcommittee in Biometrics identified in 2006 the research on sensor technology for biometrics at a distance as a 'primary research challenge' (National Science and Technology Council Subcommittee on Biometrics 2007), while one year later

the BioSecure Network of Excellence published its Biometrics Research Agenda (The BioSecure Network of Excellence 2007), calling research in distributed sensor networks and the transparent use of biometrics, requiring no actions from the end-user in supervised or unsupervised ways one of the most 'urgent' research topics. In the language of biometrics, this is described as "unobtrusive," "convenient to the user," and "transparent." The latter term especially is rather intriguing, since it refers to a characteristic of systems that in other discourses, for example that of political accountability, would be qualified in absolutely opposite terms. And, although such biometrics at a distance will not involve the body to be available in exactly the same ways as described above—to have it perform and behave in precisely circumscribed ways in order to render it machine-readable—it does not alter the fundamental assumption that bodies are available to this kind of treatment and use.

The growing extent of presumed availability is another aspect that needs to be noted, especially in light of current developments toward "under the skin" biometrics: today there are concerted, often government and EC-funded research efforts to develop new biometric concepts involving (in some cases distant) registration of brain and heart activity patterns through electroencephalograms and electrocardiograms, from which to derive a personal profile that subsequently can be used for "unobtrusive" authentication (Riera et al. 2008a, b). For example, authentication systems for high security control rooms for critical infrastructures, and for truck cabins have been developed using these techniques, based on the idea that security and safety can be enhanced by continuously authenticating who is present in these spaces or operating equipment and vehicles. Next to this, there are the investments in "new security concepts" that involve an extended set of sensors, measurements, pattern analyses and profiling techniques, focussing on pulse, body temperature, pupil dilation, gait and movement patterns, and voice pitch, in order to assess people passing through public spaces like airports (Burns and Teufel 2008). The aim is to "filter" out those deviating from a set of norms believed to distinguish the harmless and innocent from those that are not. Comparable to the ideas underlying the polygraph, certain physical indicators of arousal, stress, and so on, are believed to correlate with "hostile intent." Apart from the highly disputable assumptions concerning such correlations, or the deeply worrying potential effects of anticipatory conformity such practices may generate (Rouvroy 2009), the very idea that one can direct such sensors, and do such measurements on people, be it in public spaces or in work environments, is indicative of the extreme extent to which people's bodies are in fact assumed to be available for biometric processing.

In conjunction with the issues raised above in relation to soft biometrics—the automation of intransparent, but potentially highly contestable categorizations and classifications of gender, ethnicity, race, age, and so on—which, significantly, are equally amenable to distant operation—and a picture of technical capabilities potentially deeply affecting embodied experience emerges that clearly requires sustained critical research and assessment for years to come.

3.5 Conclusion: Critiquing Normativities in the Informatization of the Body

Summarizing the arguments made, we have seen how the assumptions of similarity and stability of human bodies and their features enact essentially contestable norms concerning normalcy and difference, which unavoidably will have more or less serious exclusionary effects. Moreover, an additional third assumption regarding the availability of human bodies for enrollment in technical configurations was identified, indicating how biometrics imposes certain norms concerning the way bodies may be demanded to comply with biometrics requirements. In discussing new developments in physiological "beneath the skin" and distant sensing biometrics, the intensification and extension of this presumed availability was described, while the development of soft biometrics was shown to entail the black-boxing and automation of essentially contestable and socio-politically highly sensitive classifications and categorizations.

Taken together, these developments signify the deeply political and normative nature of the incremental informatization of the body we witness today (van der Ploeg 2002). It is, therefore, crucial that the interdisciplinary study and analysis of the intricacies of these technologies keeps pace with these developments. Difficult though this may be, given their highly complex, formalized, abstract, and ever more deeply embedded, software-encoded character, we must continuously assess precisely which norms, which definitions, and which aspects of our embodied identities are being woven into the very fabric of our ever smarter environment.

Acknowledgments Funding of the research for this paper was partly provided by the European Research Council and the European Commission, both under the European Community's Seventh Framework Program (FP7/2007-2013), DigIDeas Project/ERC Grant Agreement 201853, and HIDE project/EC Grant Agreement 217762.

References

Akrich M (1992) The description of technical objects. In: Bijker WE, Law J (eds) Shaping technology/building society—studies in sociotechnical change. The MIT Press, Cambridge, pp 205–224

Bordo S (1993) Unbearable weight. Feminism, western culture and the body. University of California Press, Berkeley

Bowker GC, Star SL (1999) Sorting things out, classification and its consequences. MIT Press, Cambridge

Brouwer E (2007) Digital borders and real rights. Effective remedies for third country Nationals in the Schengen Information System. Wolf Legal Publishers, Nijmegen

Burns RP, Teufel H (2008) Privacy impact assessment for the future attribute screening technology project. Department of Homeland Security, Washington, DC

Castle MN (1998) Hearing on biometrics and the future of money. Committee on Banking and Financial Services, Washington

Cole SA (2006) The myth of fingerprints. Gene watch. http://www.gene-watch.org/genewatch/articles/19-6Cole.html
Den Hartog JE, Moro-Ellenberger SL et al (2005) How do you measure a child? A study into the use of biometrics on children. TNO, Delft
Duden B (1991) The woman beneath the skin, a doctor's patients in eighteenth century Germany. Harvard University Press, Cambridge
Fausto-Sterling A (2008) The bare bones of race. Soc Stud Sci 38(5):657–694
Foucault M (1975) The birth of the clinic: an archeology of medical perception. Vintage/Random House, New York
Foucault M (1977) The history of sexuality vol 1: The will to knowledge. Penguin, London
Foucault M (1979) Discipline and punish. The birth of the prison. Vintage/Random House, New York
Haraway DJ (1991) Simians, cyborgs, and women: The reinvention of nature. Free Association Books, London
Harding S (ed) (1993) The 'racial' economy of science. Indiana University Press
Hayles KN (1999) How we became posthuman. Virtual bodies in cybernetics, literature, and informatics. Chicago University Press, Chicago
Home Office Identity and Passport Service Passport Photographs. London. http://www.direct.gov.uk/en/TravelAndTransport/Passports/Applicationinformation/DG_174152
Jain AK, Lu X (2004) Ethnicity identification from face images. SPIE International Symposium on Defense and Security: Biometric Technology for Human Identification
Jain AK, Dass SC et al (2004) Soft biometric traits for personal recognition systems. International Conference on Biometric Authentication, Hong Kong
Koslowski R (2005) Real challenges for virtual borders: the implementation of US-VISIT. Migration Policy Institute, Washington DC
Lacqueur T (1990) Making sex. Body and gender from the Greeks to Freud. Harvard University Press, Cambridge Mass./London
Latour B (1983) Give me a laboratory and I will raise the world. In: Knorr-Cetina KD, Mulkay M (eds) Science observed. Sage, London, pp 141–170
Latour B (1987) Science in action: how to follow scientists and engineers through society. Harvard University Press, Cambridge
Li SZ, Schouten B et al (2009) Biometrics at a distance: issues, challenges, and prospects. In: Tistarelli M, Li SZ, Chellappa R (eds) Handbook of remote biometrics for surveillance and security. Springer, London, pp 3–21
Lyon D (ed) (2003) Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge, London
Merleau-Ponty M ((1945) 1962) Phenomenology of perception. London, Routledge and Kegan Paul
Mintie D (ed) (1998) Biometrics in human services user group Newsletter, The Connecticut Department of Social Services, 2(2)
National Science and Technology Council Subcommittee on Biometrics (2007) The National Biometrics Challenge. Washington, DC, pp 1–19
Riera A, Soria-Frisch A et al (2008a) Multimodal physiological biometrics authentication. Biometrics: theory, methods, and applications. Wiley/IEEE
Riera A, Soria-Frisch A et al (2008b) Unobtrusive biometric system based on electroencephalogram analysis. EURASIP J Adv Signal Process pp 1–8
Rouvroy A (2009) Governmentality in an age of autonomic computing. Technology, virtuality, utopia. Computer Privacy and Data Protection, Colloquium on Autonomic Computing, Human Identity and Legal Subjectivity, Brussels
Schiebinger L (1993) Nature's body. Gender in the making of modern science. Beacon Press, Boston
Star SL (1991) Power, technology and the phenomenology of conventions: on being allergic to onions. In: Law J (ed) A Sociology of Monsters: essays on power, technology and domination. Basil Blackwell, Oxford, pp 26–56

The BioSecure Network of Excellence (2007) The Biosecure Research Agenda. http://biosecure.it-sudparis.eu/AB/index.php?option=com_content&view=article&id=67&Itemid=36
van der Ploeg I (1999a) 'Eurodac' and the illegal body. The politics of biometric identity. Ethics Inf Technol 1(4):37–44
van der Ploeg I (1999b) Written on the body: biometrics and identity. Comput Soc 29(1):37–44
van der Ploeg I (2002) Biometrics and the body as information: normative issues in the socio-technical coding of the body. In: Lyon D (ed) Surveillance as social sorting: privacy, risk and automated discrimination. Routledge, New York, pp 57–73
van der Ploeg I (2003) Du Corps-matière au corps-information. La Recherche—Hors Série: Le Corps Humain de A à Z (12):36–39
van der Ploeg I (2008) Machine-readable bodies: biometrics, informatization and surveillance. In: Mordini E et al (eds) Identity, security and democracy. Lancaster, IOS Press, NATO Science Series, Amsterdam, pp 85–94
Woolgar S (1991) Configuring the user: The case of usability trials. In: Law J (ed) A sociology of monsters: essays on power, technology and domination. Routledge, London, pp 57–99

Chapter 4
Electronic Exchange of Signals on Youth at Risk: A Value Perspective

Ton Monasso

Abbreviations

VIR	Verwijsindex Risicojongeren
VSD	Value-sensitive design
ANT	Actor-network theory

Contents

4.1 Introduction 42
4.2 Value-Sensitive Design 44
4.3 Methodology: The Framework 46
4.4 Methodology Applied: Values and VIR—Case Description 48
4.4.1 Informal Institutions 48
4.4.2 Formal Institutions 50
4.4.3 Institutional Arrangements 51
4.4.4 Interactions by Actors 52
4.4.5 Technology 52
4.5 Methodology Applied: Values and VIR—Value-Sensitive Design 53
4.6 Conclusions and Reflections 54
References 55

Contribution received in 2010.

Ton Monasso is a consultant in the area of the electronic exchange of information on youngsters. This contribution builds upon his master's thesis at the 3TU. He identified fundamental considerations for decision-makers with regard to the IT-supported recognition of children with psychosocial problems.

T. Monasso (✉)
Zenc Research and Consultancy, The Hague, The Netherlands
e-mail: ton@tonmonasso.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_4,

4.1 Introduction

An estimated 3.5–12% of Dutch youngsters have a multitude of psychosocial problems, which are either directed internally (emotional problems) or externally (behavioral problems) (Zeijl et al. 2005). These problems have reached a level where they impair their social functioning and may even cause harm to others. The recognition of children with these problems can be difficult. Many of these youngsters are known by some organization, such as schools, police, youth care or sports clubs, as having a problem. However, the dispersed information often is never combined, so that the informational puzzle around a child is incomplete. Not every professional action requires that all information available elsewhere is aggregated, but combining data pieces may contribute to a better diagnosis or a better intervention. Sometimes, the combination of different concerns leads to an intervention that would not have been taken in the absence of complete information. Alleged child abuse is a good example of such a case. It is often very hard to conclude that a child is being abused, and professionals are reluctant in diagnosing this, because the consequences can be large. More certainty, by the exchange of information across organizations and individuals, hence sharpening the picture of the situation and starting or aligning interventions with the diagnosis, may ultimately contribute to the child's psychosocial health. On the other hand, this very same exchange of information can be problematic because of factors such as informational privacy risks, semantic errors, and biases in decision-making.

The Dutch risk signaling system currently (2009) under development is a centralized version of several local systems. The so-called 'Verwijsindex Risicojongeren' (VIR) collects risk signals from a multitude of disciplines. If a professional is concerned about a child, where the concern fits reporting criteria agreed on beforehand, he can issue a report in the system. The report only contains the unique citizen identification number of the youngster, the organization, and individual who issued the signal and the retention period, with a maximum of two years. No substantial information of any kind is provided. When the system receives multiple reports of a single youngster, a match occurs and the involved professionals are informed. By providing mutual contact details, the original report issuers can contact each other and discuss the case and child at hand. At the local level, arrangements have been made which often include a compulsory follow-up. At this level, the municipality also takes the initiative to select organizations that will be connected to the VIR, which can reside in four domains: police and justice, education, health, and employment services. Currently, regulation is prepared that enables professionals to report without the consent of the child or the parents. A typical event that may trigger use of the system is the molesting of a bus shelter by a child, which makes a police officer decide to enter a risk signal. If the child also skips school and a report already existed in the VIR, a match occurs, and the police officer and school should sit together to discuss the child. The system only facilitates already existing processes of diagnosis and intervention. In that sense, it

is a decision support system and only embodies a very basic technology. Nevertheless, the system has real value consequences.

Values are expressions of what actors (humans, organizations) believe is important. They can be context-dependent, but are generally formulated rather abstract. Examples of values are justice, peace, privacy, and duty towards unborn children. Values can be dependent on the actor and may depend on their interests. However, they may also have a non-selfish origin.

A practical, as well as theoretical, challenge is to design systems such as the VIR in such a way that they recognize and where possible incorporate the relevant values from the relevant actors affected. This clarifies the trade-offs that need to be made at both the political and the designers' level and make it possible to optimize the design for some values without harming others (Pareto improvement). In its essence, values are incorporated in the design criteria. Sometimes as constraints—the design should conform to a certain value—but most often as goals—the design should try to maximize the beneficial effect on this value. The art of designing with values in mind is called value-sensitive design (VSD).

In this chapter, we will apply a VSD approach to the design of the VIR, where the latter is a case study that illustrates the more general approach. The central question of the chapter is:

Which values are affected by the VIR, in what way, and how can values be incorporated in the design?

To be split in:

- Which values are affected by the VIR?
- Which design choices (examples) have value-related consequences?
- How can values be incorporated in the design of the VIR?

The first two parts of the research question are descriptive and unravel the value aspects of the VIR, the last is more prescriptive and shows how VSD can contribute to improve the design, either by taking Pareto improvements or having made an explicit and legitimated trade-off between conflicting values. This chapter leaves no room for a full discussion of the underlying case study. Hence, we will not dive into the alternative design choices, nor examine their relation to all the values. Instead, we will illustrate the use of VSD as an approach, discuss the relevant values, and will give examples of design choices that have value-related consequences.

At the heart of our case study, we conducted an extensive literature study aimed at thoroughly analyzing our case, complemented with 13 expert interviews. The group of experts was heterogeneous and primarily consisted of people fulfilling an executive responsibility, either as project leader, policymaker or practitioner. We did exclude politicians, as we think not the values as such, but their translations to and from technical and institutional choices is the greatest challenge. The framework we have chosen to support our VSD approach is an existing one from the field of institutional economics. We do not argue that this is the best framework, but we have experienced it to be useful. As such, it can serve as a starting

point for developing a more elaborate VSD methodology than has been done up until now.

We will start with a more elaborated discussion of the VSD literature. Those who are merely interested in the characteristics of the case study and not so much in the theoretical and methodological discussions on VSD, may skip this section. Next, we will introduce the framework that forms the heart of our method. Then, we will apply this method in a descriptive way, so as to be able to lay out the analytical groundwork for the prescriptive part. We will finish with conclusions and reflections.

4.2 Value-Sensitive Design

VSD recognizes that technology and institutions are interrelated. This insight runs parallel with thinking in other disciplines (e.g., Bouwman et al. 2005; Hanseth and Monteiro 1998; Koppenjan and Groenewegen 2005; Orlikowski and Robey 1991). Technology and institutions are both value-laden (Friedman and Kahn Jr 2002). Compelling examples are biases in computer systems (Friedman and Nissenbaum 1996) and classification biases (Bowker and Star 1999). The former authors define bias in the context of computer systems:

> We use the term bias to refer to computer systems that systematically and unfairly discriminate against certain individuals or groups of individuals in favor of others.

Before one can take up this notion in any design process, one must establish the possibility to deliberately influence the way in which values are inscribed into technology and institutions. The value-ladenness of institutions is covered by the field of political science, institutional economics and public administration and is much more classical and obvious than the thinking on the value-ladenness of technology. Consistent with VSD, we take an interactional position (Friedman and Freier 2005) with regard to technological determinism. We neither assume technology goes its own way (the exogenous position, Friedman and Kahn Jr 2002), regardless of human interference, but we also do not tilt to the fully embodied position, where all value effects of technology can be traced back to deliberate design choices. The interactional position is supported by three concepts or theories. First, structuration theory, built around the notion of the duality of structure (structures are both shaping and shaped by themselves), pointing at the existence of positive feedback cycles. Orlikowski and Robey adapted Giddens' structuration theory to the field of information systems (Orlikowski and Robey 1991). A competing theoretical strand is actor-network theory (ANT), which describes the inscription of desired behavior into artifacts and the translation of values in the interaction between actors within a network in a very abstract way. ANT does not a priori distinguish between technology and human actors. It recognizes resistance against change, framed as irreversibility (Hanseth and Monteiro 1998). Finally, Hughes (1994) coined the term technological momentum. He argues that technology becomes more autonomous

over time. The reverse also holds: the human influence with regard to the consequences of technology is largest in the early phases of the life cycle.

Now that the designers' influence has been explored, it is still unclear whether a designer can explicitly and adequately influence the future. Albrechtslund (2007) talks about the positivist problem in this respect. He remarks that a design can never foresee all use contexts. Bimber (1994) calls it unintended consequences, and elsewhere, we have discussed the problems of information overload, bounded rationality and non-linear behavior of complex systems (Monasso 2006). Nevertheless, complexity, uncertainty and fuzziness do not provide an excuse not to be aware of and design for values where possible.

Value-sensitive design holds a rather optimistic and promising view on the relation between values and technology. It embodies a third phase in ethics, after analytical and applied ethics (van den Hoven 2007). It is a way of thinking that can be described as:

> [P]rincipled in that it maintains that such values have moral epistemic standing independent of whether a particular person or group upholds such values. At the same time, Value-Sensitive Design maintain that how such values play out in a particular culture at a particular point in time can vary, sometimes considerably. (Friedman and Kahn Jr 2002)

We do not fully agree with the assumption of epistemic independence. It may be that most values are generic, but when designing systems, one has to make trade-offs between values. It is in this process that ideologies or other ways through which moral stance is expressed may support the process of decision-making. If one only formulates values such as fairness and justice, one has escaped these difficulties by fleeing to a higher level of abstraction. We think that explicating these trade-offs is essential. Next, moral theory may come in, to take a stance in these dilemmas, a process that is not directly part of a VSD methodology or at least is not unique for design of technology. After the moral stance has been taken, VSD insights may be used to incorporate the value in the design.

Our analysis of values is a form of disclosive computer ethics, which can be distinguished from mainstream computer ethics (Brey 2000). We try to uncover moral issues beyond the actual usage of technology by humans and instead focus on the design phase. Brey states that such an analysis can remain largely pretheoretical, using only loose definitions of moral values, if one is not willing to depend of a particular moral theory. Indeed, we will not choose a moral viewpoint, but try to identify values in general. Nevertheless, this still does not encompass a full VSD cycle, as one has to decide on trade-offs. Disclosive computer ethics therefore comprises only the first step and the descriptive part of this paper.

VSD is promising, but its methodology is not mature yet (Flanagan et al. 2005). Several contributions, from different fields, have been made, among which are values in design (Flanagan et al. 2005)—which draws upon the triad discovery, translation, and verification—and critical technical practice, a methodology aimed at bridging the world of cultural reflection and design, which may also be applied to values in technology (Boehner et al. 2005). Some people consider value-sensitive design as a specific methodology, next to values in design, critical technical

practice and others, because Friedman and others—who coined the term VSD—have also made methodological contributions (e.g., Friedman et al. 2001), where they distinguish conceptual, technical, and empirical investigations). Nevertheless, we observe that VSD is conventionally referred to not as a methodology, but merely as a generic approach, a goal. Hence, we use VSD as a generic term and distinguish several methodological contributions in it.[1] Earlier contributions in the field are useful, but have not systematically combined institutions and technology in their analysis. Moreover, they generally lack rigor and, as such, can structure an analysis, but do not provide much guidance on its contents. We would like to add a methodology aimed at providing this guidance. As research proceeds, we expect the VSD field to be able to validate, compare, recombine, and improve different methodologies. At this moment of time, the number of case studies and degree of detail of the methodologies, does not allow for systematic comparison.

4.3 Methodology: The Framework

Since no 'ready-made' framework from the field of VSD is available to support the analysis of our case, we will have to use one from a different scientific discipline, which can be used without much alterations. This still is a process of methodological development, since that framework was not primarily intended for this purpose. Developing a framework has both theoretical and practical relevance. 'Design' is on crossroads: a design process leads to the creation of artifacts, but it can be inspired by and based upon theory. We regard VSD theory to be aimed at prescription, as design is creational by definition.

The exchange of personal information in the public domain requires thoughtful consideration of institutional aspects, beyond the technical, as many actors are involved and multiple, often contradictory values should be taken into account. Therefore, at the core of our analysis, we use a framework that is explicitly developed for socio-technical systems, characterized by unruly technology, the involvement of multiple parties, both public and private, the existence of market forces and government regulation (Koppenjan and Groenewegen 2005). The market forces are not that relevant in our case, but the other characteristics match the definition of the exchange of sensitive information in the public domain.

Our analytical framework is borrowed from Groenewegen (2005), who extended Williamson's framework from the field of institutional economics (1998) with a technology element. The visual representation is given in Fig. 4.1. Four elements deal with institutions and are based upon Williamson's framework. Each of them operates at a different level of analysis. The upper level comprises informal institutions and is hardest to change, the lowest one deals with the interactions

[1] Manders-Huits and Zimmer 2008 use the term 'value-conscious design' to refer to the overall approach, and regard value-sensitive design as a specific one.

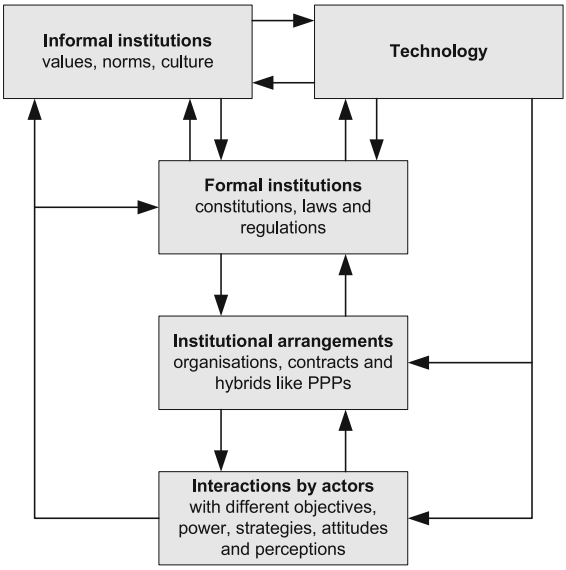

Fig. 4.1 Groenewegen's framework (2005)

between actors and can be changed more easily. Depending on the time scale and the resources of actors, elements could be considered either as constraints or as instruments for a particular actor.

All relationships between the original four elements are bidirectional. Informal institutions shape formal institutions, as formal institutions shape institutional arrangements and so on. The other way around, behavior can also induce a change in institutional arrangements, the arrangements may lead to new or modified formal institutions etc. Next to these elements, Groenewegen (2005) introduced technology.

The framework is still in its infancy. We do not agree with the positioning of the technology, its aggregation level, or with the way the relationships are depicted. By placing technology next to informal institutions, it seems that technology is very hard to change. We think technology resides at different levels of abstraction and fluidity. It should be placed on a more equal analytical footing with institutions, which have been split up into four elements. Technology can be thought of as concrete instances interacting (at the lowest level), as creating networks of functionality (comparable to institutional arrangements), to constrain behavior by technical standards and architectural choices, and finally, by the availability of fundamental scientific knowledge (at the level of informal institutions) (Kunneke 2008). If placed on these levels, it is interacting with all elements of institutions, as well as with other technological levels. Moreover, we would not limit the relevant relationships beforehand, as we think, for every combination of analytical elements, one can envisage a more or less direct relation. Although we comment on the model, we consider it more useful to apply it to our case and explore whether its fundamentals contribute to VSD methodology, than to carry out a theoretical

exercise in adapting it without investigating its fit for our purpose. We use the framework for two reasons: to assist in identifying relevant aspects, and facilitate layered thinking.

The variety in elements allows for the embodiment of and discrimination between different types of biases, following the classification of Friedman and Nissenbaum (1996). Pre-existing biases are mostly of an institutional nature, technical ones can be located in the technology element, and emergent biases will mostly be present in the interactions between actors or the technology. The way in which the elements can be used to explore value-laden consequences of design choices, will be shown in our discussion of the case study.

4.4 Methodology Applied: Values and VIR—Case Description

We will apply Groenewegen's framework to a single case study: the Dutch national risk signaling system for children with psychosocial problems. We will first discuss the problem domain, and then consequently apply the five elements of the framework to identify biases and other value consequences. Many themes can be located in more than one element of the framework. For reasons of simplicity, we only discuss them once.

We will start our analysis from the top down, as it is easier to discuss the elements with the most constraining effect at the beginning. Our conceptualization of Groenewegen's framework is shown in Fig. 4.2. With conceptualization, we mean an overview of the relevant notions we encountered during our exploration. It is the result and not the starting point of our analysis.

We start with the informal institutions section. This element is the one where the relevant values have to be explicated. After that, we discuss the other elements subsequently. The analysis is a narrow selection of a more in-depth study into information systems that support the recognition of children with psychosocial problems (Monasso 2008).

4.4.1 Informal Institutions

Three values play a central role in this system. First, the successful development of children, which can be read as the absence or mediation of psychosocial problems. Second, moral autonomy, which is the ability of individuals to make their own choices in life, relying upon their own conception of a good life. Third, the absence of information abuse, which equal the wish that personal and sensitive information is not being consciously abused by other actors for their benefit. These values are depicted in Fig. 4.3, which also shows the actors that hold them. As will become clear in the remainder of this analysis, the values can be contradictory and a trade-off exists, most notably between the child's development and privacy. The figure

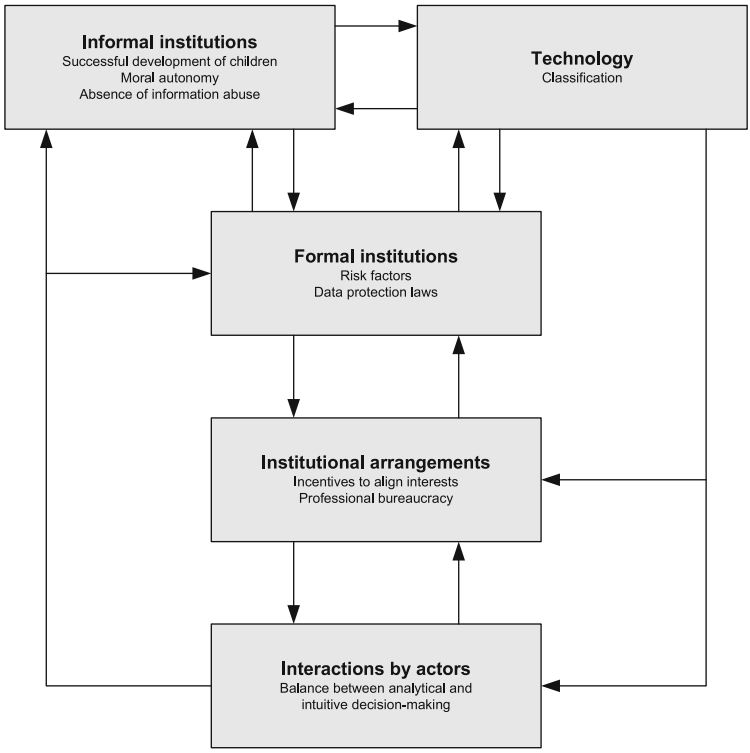

Fig. 4.2 Simplified conceptual framework

also shows that many effects are the result of intervention in the life of the child or its family. The ultimate goal of the VIR is to intervene in those situations where that is needed and helpful. Information collection is only a means to an end. Although the intervention part is not analyzed separately in this chapter, this clearly needs to be taken into account (as a given or as a set of design choices) when designing for the VIR.

The privacy values are affected by the quantity and the type of data that is collected, processed, and stored in the VIR, as well as measures taken to constrain these activities. It is ultimately dependent on choices in the other elements, and is a 'given' for designers, since they cannot influence the existence of the values themselves.

The trend in Dutch society is to attach more weight to the successful development of children, and consequently less to privacy and absence of discrimination. This shift has been influenced by some individual dramas that received much media coverage. It is an illustration of the only way in which values may change radically instead of incrementally: when some 'crisis' occurs, mostly an event that makes people rethink their moral position. In this case, new information was

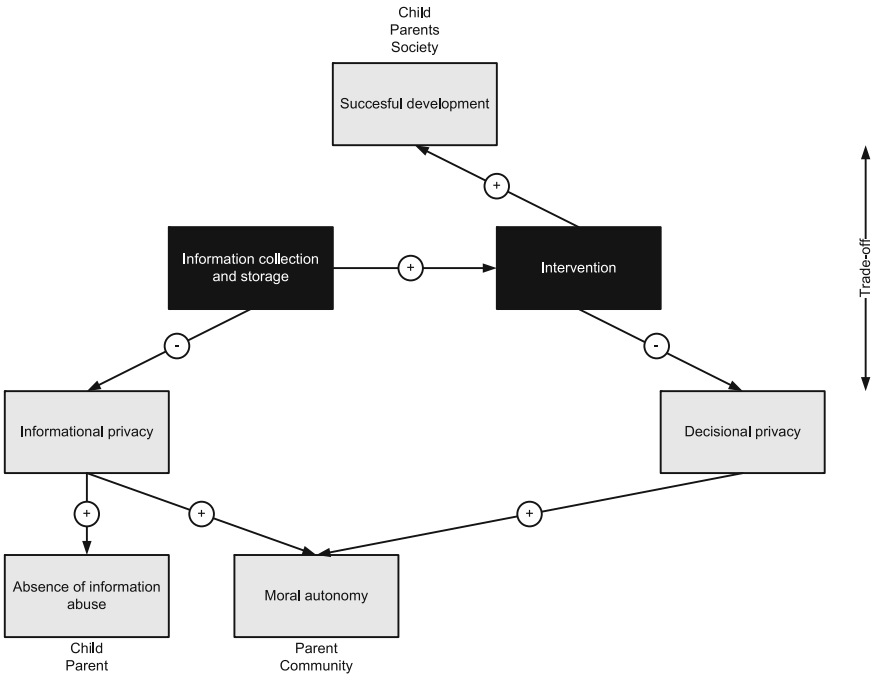

Fig. 4.3 Simplified relationships between normative demands and intensity of information collection and storage and intervention

offered to the public and politics, that was often not known to them before, which 'activated' the importance of successful development of children. Probably this always has been a latent value, but its importance in the context of government policy and information systems has only become manifest after the incidents.

4.4.2 Formal Institutions

Formal institutions have a bidirectional relationship with values. Laws and regulations can contain biases or they can codify certain interests, such as the protection of the child. Often, formal institutions are the result of moral discussions on the desirability of (types of) intervention. A striking example in our case is the usage of risk factors.

Biases may be introduced in a conscious and systematic way if one decides to use risk factors to discover children with a high likelihood on present or future psychosocial problems. Risk factors are group characteristics such as low family income, low parental education, and also teenage pregnancy or foreign origin (Brown et al. 1998; Deković 1999; van IJzendoorn et al. 2007). In all cases, the

factors have been derived from statistical correlations and not all results can be generalized to other contexts. In no way, they point to individual causal relationships. This type of relationship has been framed as correlative inferences (Birrer 2005) or non-distributive generalizations (Vedder 1999). Risk factor research has indicated a long list of factors that may point to, for instance, child abuse or criminal behavior during adolescence. Often, the concurrence of at least three of four risk factors points to increased likelihood on problems, sometimes even with a factor seven compared to a situation in which no risk factors are present. Risk factors may be codified in the reporting protocols, but they also exist implicitly in the heads of professionals. They often have to make intuitive decisions where their own impressions and experience plays a role. These individual decisions can have characteristics of a (moral) black box.

Relevant laws and treaties are mainly in the sphere of data protection. Without an explicit legal basis or the consent of the child or his parents, the European and Dutch privacy data protection regulations do not allow the storage, let alone the exchange, of sensitive data such as those stored in the VIR. The data as such are not sensitive, but the context in which they exist, provides additional meaning.

4.4.3 Institutional Arrangements

At the level of institutional arrangements, one is concerned with the set of organizations and the allocation of tasks, and responsibilities among them. Two theoretical strands are highly relevant here. First, principal-agent theory (Douma and Schreuder 2002) gives a perspective to analyze whether the interests (aligned with values) are carried out by agents, which we consider to be human actors, or whether the enactment of these values is perverted by disturbing influences. We found that, in those municipalities where a VIR-like system already exists, the amount of reports issued in a particular period heavily depends on the dominant media attitude in that period. When child abuse numbers flushed the newspapers, the number of reports expanded, but when government data leakage was front-page news, the numbers fell sharply. This means that the reporting criteria alone do not fully guide the reporting process, but that factors such as personal moral stance and the fear for liability also play a role. If organizations are perceived as agents, bureau politics is likely to come into force.

Organizational theory is a second strand of knowledge. Most of the organizations connected to the VIR are a form of professional bureaucracy (Mintzberg 1983). This kind of organization leaves much room for individual discretion and is hardly accessible to outsiders. In many professional domains, of which the medical discipline probably is the most notable example, professional values strongly influence behavior. Think about a psychologist who treats adults who have been victim of child abuse themselves. Their own experiences increase the chance that their children are also abused. They may even confirm this during therapeutic sessions. However, the psychologist has a professional and confidential

relationship with the parents, and not with the children associated. Often, they do not issue a report, because their professional value is the treatment of the individual patient in a sphere of confidentiality and not the health of 'outsiders'. Even when these values are not directly codified, or the law explicitly creates exemptions, professional values may dominate others.

4.4.4 Interactions by Actors

From the field of behavioral psychology, we can learn about the difference between analytical and intuitive decision-making. Both forms carry their benefits and drawbacks. Hammond's continuum aligns the task environment with judgement characteristics, and therewith provides a contingency theory (Daniel 2003). He prescribes that in a situation where much information is available, with multiple cues and a high time pressure, intuition is better suited than analytical decision-making. When a narrower decision has to be made, the number of cues can be reduced and appropriate models are available, analytical decision-making is the preferred form. An advantage of analytical decision-making is that it partially corrects for fundamental human cognitive biases. Several biases exist in human judgement (Munro 1999; Raiffa et al. 2002). We may overrate the value of new evidence, of first impressions, we try to fit new material into our already existing perception instead of revising our thoughts, we have problems in correctly translating statistical correlations to real world situations and trade-offs, and so on. With these biases in mind, one can design a system that either does not reinforce them, or even better, tries to compensate for it. The VIR does not exchange substantial information, which may result from thinking about biases. Consider the (selective) exchange of information attached to a report. The first impression can be very sticky, whereas the problem situation may be very complex and the issuer of the report is not a skilled writer, but only typed a short memo. This impacts the perception of the other professional and harms a good diagnosis.

Analytical models compensate for these biases, but they also introduce new ones. Especially since models are often used across the full range of a discipline, small errors often have large consequences, compared to the large error in an individual case. We would say that analytical models have a high risk of introducing systematic errors and hence create bias as defined in the beginning of this paper.

4.4.5 Technology

The exchange of data by means of information technology requires some form of structure. Fully unstructured data exchange is not much more than the transmission of a box of unsorted papers from one place to the other. Only when some structure

is provided, meaningful exchange and analysis may take place. In structuring information, one often makes use of classifications. The design of classes and the way residual categories are handled affect our values (Bowker and Star 1999). For instance, if a capable and well-resourced mother who gave birth to her child at the age of 23 is labelled as teenager, she and her child may fall in the high-risk category teenage pregnancy, together with a 15-year old mother who originated from a problem family herself. The categories have independent meaning over the individual cases they contain. Again, the danger of non-distributive generalizations exists.

4.5 Methodology Applied: Values and VIR—Value-Sensitive Design

Now that we have identified several elements of an institutional and technical design that impact upon our values, we can use this as a starting point to design with values in mind. This design is conscious and explicit, and gives values, the weight of 'criteria' that are used to objectively determine (*ex ante* and *ex post*) and normatively assess the outcome of the design. We will present three examples of designing for values, which are all adaptations to the currently envisaged VIR. Two of them are dilemmas (trade-offs), one of them suggests a Pareto improvement.

A first dilemma concerns the use of risk factors, discussed in Sect. 4.3. The advantage of risk factors may be that professionals are supported in their awareness of looking for potential problems. Compare this with a tourist being more cautious in the townships of Soweto than at a Berlin park: one is alarmed by the characteristics of the 'environment.' It may contribute to objectivity, since the factors follow from research.

However, the use of risk factors may bring several drawbacks with it. It may lead to systematic over-reporting of children from immigrant parents, to whom multiple risk factors may apply. Second, the concurrence of risk factors often does not indicate a risk higher than 25% that some undesired consequence may be(come) present. If consequently applied to a large group, it may be that four times as many people are labelled as high-risk cases, than there are cases where something is actually wrong. Stigmatization of whole groups along the lines of ethnic origin may be the emergent result of a well-intended use of risk factors to care for children's psychosocial development, resulting in a restriction of moral autonomy. Third, risk factors may introduce a new blind spot for those situations where children are at risk, but no risk factors are present. Over-reliance on pseudo-objectivity should be prevented.

The dilemma is in the successful development of children versus the moral autonomy of parents. One may legally prohibit the use of risk factors if one gives priority to the latter, but then one also loses its contribution to better recognition. Another way is to facilitate training and awareness, so that risk factors are used in

an appropriate way. Next, reports which have been issued based on the criteria of the concurrence of risk factors may be labelled differently, so that the receivers of a matched report are aware of its origin and can be more critical in assessing its value. Finally, one may use management information to check how risk factors are applied, to check whether the concept as such has benefit in the context of a VIR.

A second dilemma is in the 'degree of interventionism' that follows from the VIR. One may choose for a system that comprises a small number of children with a relatively high average risk on psychosocial problems, or a broad system where the average risk is consequently smaller. The design factor is the reporting barrier: how severe should the signals of potential problems be, to allow reporting in the VIR? One may suggest that more signals equal a higher chance on helping (more) children. On this point, some experts warn that we should not intervene too much—it may harm instead of helping the child (Breeuwsma 2009; Weijers 2007). Moreover, the chance on intervention in relatively light problem situations may be higher, impacting upon the moral autonomy of the family.

Here, the dilemma can partially be escaped by making sure the follow-up of matches in the VIR always is a thorough professional assessment, where the option not to intervene should be considered. Designers can influence this in communication on the system and in the development of protocols. In any case, the system should be used as a tool to act in the interests of the child and not become a bureaucratic substitute for professional responsibility.

A possible Pareto enhancement follows from the discovery that the way design choices impact upon the successful development of children as a value is not always clear. Like the previous dilemma (too much intervention), one may severely disagree on what is beneficial and what is not. It may be helpful to install 'value watchers,' who guard the process of design, implementation, usage and evaluation of the VIR in the interests of the child. An advisory board, dedicated to this task and not to the difficult trade-offs with other values, may clarify the 'technocratic' side of the design. If there is a lack of information on the effects on a certain value, it may be very hard to effectively design for values.

4.6 Conclusions and Reflections

We have identified three relevant values that are affected by the VIR: the successful development of children, moral autonomy and the absence of information abuse. We have seen that these values are often contradictory and a trade-off needs to be made. Our approach, in which we borrowed a framework from a 'strange' discipline, made it possible to analyze the relevant values, design choices and their interrelationships in a structured way. Based on those insights, designers are supported in adjusting their design so as to optimize for the relevant values. The VSD methodology does not lead the way to the outcomes of the design, but identifies the trade-offs (which are normative and need to be made in the 'political' arena) and may suggest Pareto improvements.

We have seen that a system such as the VIR needs to be put in a social and institutional context, and that its effects on values not only depend on technology. Formal institutions, institutional arrangements, and the actual interactions by actors are part of the context and can be often be influenced by design. That is, if we conceive design in a broad way. Legal specialists drawing up new legislation are no less designers than are engineers. The framework, and the VSD approach as such, may contribute to interdisciplinary cooperation, because its fundamentals are not grounded in a specific traditional discipline. Just like design is an interdisciplinary activity, the development of VSD as an approach needs the involvement of ethics philosophers, engineers, legal specialists, economists, psychologists, and others.

References

Albrechtslund A (2007) Ethics and technology design. Ethics Inf Technol 9(1):63–72

Bimber B (1994) Three faces of technological determinism. In: Smith MR, Marx L (eds) Does technology drive history? MIT Press, London, pp 79–100

Birrer FAJ (2005) Data mining to combat terrorism and the roots of privacy concerns. Ethics Inf Technol 7(4):211–220

Boehner K et al (2005) Critical technical practice as a methodology for values in design. Paper presented at the annual meeting on computer human interaction

Bouwman H et al (2005) Information communication technology in organizations: adoption, implementation, use and effects. Sage, London

Bowker GC, Star SL (1999) Sorting things out classification and its consequences. MIT Press, New York

Breeuwsma G (2009) Kind wordt te weinig met rust gelaten. NRC Handelsblad, 26 May

Brey P (2000) Disclosive computer ethics. Comput Soc 30(4):10–16

Brown J et al (1998) A longitudinal analysis of risk factors for child maltreatment: findings of a 17-year prospective study of officially recorded and self-reported child abuse and neglect. Child Abuse Negl 22(11):1065–1078

Daniel RS (2003) Disciplined intuition: subjective aspects of judgment and decision making in child protective services. Texas A&M University, College station, Texas

Dekovi M (1999) Risk and protective factors in the development of problem behavior during adolescence. J Youth Adolesc 28(6):667–685

Douma S, Schreuder H (2002) Agency theory. In: Douma S, Schreuder H (eds) Economic approaches to organizations. Financial Times/Prentice Hall, Amsterdam

Flanagan M, Howe D, Nissenbaum H (2005) Embodying values in technology: theory and practice (draft). In: Hoven M, van den Weckert J (eds) Information technology and moral philosophy. Cambridge University Press, Cambridge

Friedman B, Freier NG (2005) Value sensitive design. In: Fisher KE, Erdelez S, McKechnie EF (eds) Theories of information behavior: a researcher's guide. Information Today, Medford, pp 368–372

Friedman B, Kahn Jr PH (2002) Human values, ethics, and design. Human factors and ergonomics, pp 1177–1201

Friedman B, Nissenbaum H (1996) Bias in computer systems. ACM Trans Inform Syst 14(3):330–347

Friedman B, Kahn Jr PH, Borning A (2001) Value sensitive design: theory and methods. University of Washington, Seattle

Groenewegen J (2005) Designing markets in infrastructures: from blueprint to learning. Delft, TU Delft
Hanseth O, Monteiro E (1998) Understanding information infrastructure (unpublished book). Available at http://heim.ifi.uio.no/∼oleha/Publications/bok.pdf
Hughes TP (1994) Technological momentum. In: Smith MR, Marx L (eds) Does technology drive history?. MIT Press, London, pp 101–113
Koppenjan J, Groenewegen J (2005) Institutional design for complex technological systems. Int J Technol Policy Manag 5(3):240–257
Kunneke R (2008) Institutional reform and technological practice: the case of electricity. Ind Corp Chang 17(2):233
Manders-Huits N, Zimmer M (2008) Values and pragmatic action: the challenges of engagement with technical communities in support of value-conscious design (working paper)
Mintzberg H (1983) Structure in fives: designing effective organizations. Prentice Hall, Englewood Cliffs
Monasso T (2006) I don't know what I'm doing. Mekelessay 2006. Delft, TU Delft
Monasso T (2008) Policy considerations for the use of IT-supported recognition of children with psychosocial problems (unpublished work). Delft, TU Delft
Munro E (1999) Common errors of reasoning in child protection work. Child Abuse Negl 23(8):745–758
Orlikowski WJ, Robey D (1991) Information technology and the structuring of organizations. Inf Syst Res 2(2):143–169
Raiffa H, Richardson J, Metcalfe D (2002) Negotiation analysis the science and art of collaborative decision making. Harvard University Press, Cambridge
van den Hoven J (2007) ICT and value sensitive design. Int Fed Inf Process 233:67
van IJzendoorn MH, et al. (2007) De Nationale Prevalentiestudie Mishandeling van Kinderen en Jeugdigen (NPM-2005). Den Haag, Wetenschappelijk Onderzoeks- en Documentatiecentrum
Vedder A (1999) KDD: the challenge to individualism. Ethics Inf Technol 1(4):275–281
Weijers I (2007) Het gaat best goed met de jeugd. Grijp beperkter en gerichter in. NRC Handelsblad, 29 September
Williamson OE (1998) Transaction cost economics: how it works, where it is headed. The Economist 1:146
Zeijl E et al (2005) Kinderen in Nederland. Den Haag, Sociaal en Cultureel Planbureau

Chapter 5
Regulating Invisible Harms

Noëmi Manders-Huits

Abbreviations

IDM Identity Management Technology
VCD Value-Conscious Design

Contents

5.1 Introduction 58
5.2 The Epistemic Gains of Identity Management 59
5.2.1 Power 60
5.2.2 Fecundity 60
5.2.3 Speed 61
5.2.4 Efficiency 61
5.2.5 Reliability 61
5.3 Accumulative Harm 62
5.4 Regulating Invisible Harms 69
5.5 Conclusion 71
References 71

Contribution received in 2010.

Noëmi Manders-Huits (✉)
3TU Centre for Ethics and Technology, Delft University of Technology, Delft, The Netherlands
e-mail: N.L.J.L.Manders-Huits@tudelft.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_5,

5.1 Introduction

As a result of the expansion of the public domain to a global level and the mobility within, there is an increasing need for identification and identity management. For this reason, Identity Management Technology (hereafter IDM) is deployed. IDM is developed for the purpose of administration and management of user entities associated with information systems, networks, and infrastructures. It forms the foundation on which access control is based (Benantar 2006, p. 2). A prerequisite for the use and application of IDM is the ascription of an 'identity' to each individual or actor, for assigning duties and responsibilities. This identity is a unique referring token used for the identification of the information system user in question.

In the fairly standard account, IDM is also sometimes referred to as 'Access Management.' In this sense it controls the access and restrictions of 'identities' (individuals as well as groups) to their rights, entitlements, opportunities, and accountabilities. In its most elaborate form, IDM encompasses the total of all means necessary in an organization or structure for electronic data processing, including user names, preferences, and access to services and applications. There is however, a related, but broader sense in which IDM can be read, and that is the sense I am alluding to in this chapter. It also affects the registration and identification of persons; in this sense IDM is concerned with the collection of identity related data and the management hereof.

This chapter will take a closer look at the benefits and harms of deploying IDM for e-government. Although rarely recognized, IDM issues are connected to issues of justice: identification is closely related to the design and management of a liberal democratic society. Following from John Rawls' principles for the design of a just society, in order to be able to provide and safeguard freedom and equal opportunities for all, one of the tasks for government is to identify and 'manage' its citizens and their needs (Rawls 1971, 1993). The tension between personal interests and the common good (individual vs. collective wellbeing) is precisely what is at stake in promoting justice and fairness in society; for example, by knowing who is a potential threat to public safety or who is in need of special care or treatment. The (moral) responsibility of government to promote and maintain the common good of society, or what I call 'care perspective,' therefore requires the identification of (individual) persons or citizens.

The issue of free-riders in society, i.e., the temptation for individuals not to take their fair share in producing or arriving at a public good, warrants identification as well. Rawls explains how collective action and free-riding go hand in hand:

> [W]hatever one man does his action will not significantly affect the amount produced. He regards the collective action of others as already given … If the public good is produced his enjoyment of it is not decreased by his not making a contribution. If it is not produced his action would not have changed the situation anyway. (Rawls 1971, p. 267)

The apparent 'it doesn't matter what I do' in-effect of one's actions (in a large enough society) may lead people to evade their public duties or responsibilities. Rawls argues for governmental enforcement in this case: If we are all moved by

the same sense of justice, the monitoring of such collective agreement should only be rational (Rawls 1971, pp. 267–277). This by implication involves the identification of citizens; yet paradoxically, it thereby also threatens certain public goods protecting the personal sphere of life such as privacy, trust, and freedom. I shall discuss this in more detail below.

The registration and regulation of identities, and associated rights and duties have a long history; the need for identity management in the capacity of administrative systems in administration and government has been around for centuries. Well-known examples of identity management systems associated with government and administration are the national population's counts, such as the Census in the United States and the 'Gemeentelijke Basisadminstratie' (GBA) in The Netherlands. In these systems, individual citizens are registered and uniquely identified by a number, a name, date of birth, and this information is replenished, depending on the system, by much more.

In the contemporary networked world, people interact with multiple identity-based organizations on a daily basis. There is also a growing trend in the casualness and degree to which individuals are treated on the basis of their acquired identities; the treatment they receive, the things they are entitled to, their rights, accountabilities, the opportunities they are given and the limitations that are imposed upon them, are shaped by the way their identities are construed and used.

IDM provides government with means for registering, monitoring, and communicating with citizens, in order to perform large-scale complex government service provision tasks efficiently and effectively. In doing so, there is a task for government to find a way of dealing with the tension mentioned above between the identification of citizens and their desired anonymity. Notwithstanding this challenge, IDM tools provide an effective way for communicating with citizens and executing governmental tasks.

This chapter is an appraisal of IDM for e-government. First I evaluate its success in terms of generating and structuring valuable knowledge for (e-)government practices in comparison with traditionally available epistemic tools. There are at least five good epistemic reasons for adopting IDM, as I will demonstrate by applying Alvin Goldman's criteria for evaluating the epistemic success of social practices. In what follows, I explore the possible risks for such 'informational' structuring of public administration and monitoring of citizens. I will focus in particular on the potential of what Joel Feinberg has coined 'accumulative harm' (Feinberg 1984, pp. 225–232), connecting to the virtually invisible risks of collecting and processing personal or identity related data.

5.2 The Epistemic Gains of Identity Management

Alvin Goldman has set out five criteria to evaluate how well different social practices lead to true beliefs. These criteria are power, fecundity, speed, efficiency, and reliability. In this connection Paul Thagard has argued that the Internet is by its

communicative nature, a social practice invoking epistemic beliefs.[1] This, I would add, also holds for other IT-practices. The beliefs implicated in these practices can be about anything, and in the case of IDM they will mostly be about persons and their identities. Thagard points to the 'veritistic' aim of Goldman's criteria:

> [P]resupposing that science aims at and sometimes achieves truth understood as correspondence between beliefs and the external world. (Thagard 2001, p. 6)

For the purpose of evaluating the epistemic success of IDM, I would like to subscribe to this veritistic aim, holding the presupposition that what is sought in IDM are beliefs about a certain person (identity related data), corresponding with other information about this person in the external world, conceivably for other purposes. What we are examining here is the way IDM contributes to the acquisition of knowledge about persons.

5.2.1 Power

The first criterion for evaluation is 'power,' i.e., the ability of a practice to help people find true answers to the questions that interest them. In case of IDM and e-government, this interest comprises the registration of persons and the regulation of their rights and accountabilities. It finds expression in the execution of governmental tasks and responsibilities, that is, by providing services to citizens in a broad sense; consider the communication of (e-)government with citizens and the providing for opportunities for their participation. IDM broadly construed, possesses this epistemic power par excellence. The very nature of this technology is to enable the management of a legion of identities with associated rights and accountabilities, and to make sure these identities (individuals as well as groups) find access to their entitlements.

5.2.2 Fecundity

The fecundity of a practice is its ability to lead to large numbers of true beliefs for many practitioners, i.e., many true believers. Needless to say, IDM improves the very fecundity in the sense of providing useful information about citizens and services to many government practitioners, since an IDM infrastructure enables multiple practitioners to access the same information at the same time. It is no longer necessary to demand information from other departments, causing delays in service and epistemic dependency on others to provide the correct and proper information.

---

[1] Jeroen van den Hoven also mentions Goldman and Thagard's work in connection with the Internet in van den Hoven 2000, p. 144.

5.2.3 Speed

The speed of a practice is how quickly it leads to true answers. Compared to the speed of getting the required information by using former methods of organizing and supporting governmental practices, the speed of using IDM exceeds these methods by far. Because IDM provides an informational infrastructure, enabling the linking of diverse kinds of information, grouped in various preferred ways, the amount of time spent in organizing the required data for each specific task is reduced to a minimum. Instead of setting up ways to getting the required information for each specific outset at the right time (and the organizational challenges that come with this), such time-consuming practices are eliminated and replaced by the use of an IDM infrastructure. What is more, the very speed of looking up information with the help of information technology, exceeds the speed of humans doing the same.

5.2.4 Efficiency

Efficiency is how well a practice limits the cost of getting true answers. By reducing human effort in searching, organizing, and structuring information (that is, because of fecundity and speed), the direct costs of doing so are also reduced. However, the indirect costs such as the costs of designing, buying, and maintaining an IDM infrastructure also need to be taken into account. As a result, there is a break-even point above which IDM is far more efficient.[2] Especially for large institutions and organizations such as governmental institutions—for example at a European level—this point can be calculated and weighed against other mid- and long-term investments.[3]

5.2.5 Reliability

The reliability of a practice is measured by the ratio of truths to total number of beliefs fostered by the practice. In the case of IDM, this criterion is, similar to the case of the reliability of information on the Internet (Thagard 2001), perhaps the most challenging of all. In his assessment of the epistemic contributions of the Internet to scientific knowledge, Thagard shows that the Internet has severely diminished the mistakes associated with print or hand-copying. At the same time,

[2] Below this point it may compete with other epistemic practices.

[3] What we have not discussed here regarding efficiency is the term 'true' in its definition; however, this will be discussed below when we speak of the reliability of the acquired information.

the Internet has increased the possibilities for critical reflection on content and its associated revisions (Thagard 2001, p. 10). It has made information available on an even larger scale than the printing press—almost ubiquitous—enabling continuous revision from a much wider public, as in the case of 'wiki's.' Yet this is also what constitutes a risk: The large-scale accessibility and the extended availability and spreading of information has increased the degree of 'data pollution.' For example when incorrect and poorly-formed data has been added to a database, this complicates its monitoring and review. Nonetheless Thagard emphasizes that knowledge-acquisition is a largely social enterprise (Thagard 2001, p. 10). This entails that although it has become more difficult to safeguard or monitor the quality of information, the increase in scale has also caused an increase in feedback from a multitude of perspectives, adding to its overall critical review.[4]

The epistemic reliability in case of IDM for e-government is also affected in another way. By communicating directly with citizens and enabling them to enter and/or verify their own personal information in government databases, the opportunities for unintentional mistakes vis-à-vis traditional government practices are diminished. Notwithstanding that citizens can also make mistakes (be it intentionally or not) when entering their own personal data, they are evidently better acquainted with this information and therefore (presumably) less likely to make mistakes. What is more, IDM provides for the possibility of linking this information to information already available on a data subject, for instance in other government databases, as a result of which the information can be verified.

In keeping with Goldman's standards of power, fecundity, speed, and efficiency, IDM surpasses former (non-technological) methods by far. The final criterion, reliability, also shows great advantages, yet calls for a cautionary attitude towards the quality of information in such informational infrastructures. In conclusion, the evaluation of epistemic success of information technology—especially IDM—for e-government demonstrates an overwhelmingly positive outcome in favor of deploying IDM. The remainder of this chapter will explore some of the harms or risks associated with the use of IDM for e-government. I will focus especially on what I call 'accumulative informational harm,' i.e., the harm resulting from the accumulation of seemingly harmless bits of information(-gathering).

5.3 Accumulative Harm

Harms associated with any technology appear in many ways; they can be visible (overt) or invisible (covert), individual or collective, direct or indirect, diffuse, e.g., as the result of a chain of events eventually leading to harm. Moreover, harms are

[4] This is especially relevant in open infrastructures such as the Internet, and perhaps to a lesser extent in secured infrastructures used for e-government; nonetheless, the entering, monitoring, review, and linking of information leads to similar issues concerning the quality of information.

often not 100% likely to happen, in which case they are framed as probabilistic harms, or risks. In the case of the use of IDM for e-government, there are numerous harms we can imagine:

- Harm inflicted through malicious intent by government, e.g., the manipulation of an IDM infrastructure in order to exercise power in relations between government and citizens (for instance by excluding a certain group of citizens, or complicating access or procedures);
- Harm inflicted through recklessness by government, e.g., the deprivation of (a group of) citizens as the result of a careless implementation of IDM;
- Harm inflicted through malicious intent by the individual who enters the data, e.g., manipulation of the system by means of identity fraud;
- Harm inflicted through recklessness by the individual, e.g., registering incorrectly by mistake, thereby polluting the database and effecting future decisions regarding services.

These examples indicate that in most cases of harm, there is an underlying assumption that the victims or perpetrators of harm are (ultimately) readily identifiable. Harm however, occurs regardless of us knowing who the victims or perpetrators are. In current discussions on intergenerational justice,[5] harm that is possibly inflicted on non-existent, future (generations of) persons is one of the recurrent themes. If we assume that 'actions or policies can only be wrong if they harm particular humans or non-human animals,' now or in the future, this is referred to as an 'identity-dependent' or 'harm-based' account (Page 2006a, pp. 132, 134). The problem for such an account is to deal with what is called the 'non-identity problem,'[6] holding the view that there is no harm where there are no persons (directly) harmed. As explained by Edward Page in the context of the intergenerational justice discussion, the actions or policies leading to harm are at the same time the '… necessary conditions of these people coming into existence (Page 2006a, p. 132).[7] It therefore involves, as put by Derek Parfit 'personal identit[ies] in different possible histories of the world.' (Parfit 1987, p. 351)

In what follows, I discuss a covert, identity-independent type of harm: a harm not resulting from malicious intent or recklessness regarding a particular person or a collective, neither resulting from obviously wrongful or harmful conduct. What I will discuss as a possible harm in the context of IDM and e-government is what I call 'accumulative informational harm.' For this I draw on Joel Feinberg's notion

[5] Cf., Laslett and Fishkin 1992 and Page 2006b.

[6] For challenging cases on this topic, e.g., resource depletion and the unborn child of a 14-year old cf., Parfit 1987. See also Cohen 2009 for a discussion of claims to compensation for a wrong that was also a condition of a person's existence.

[7] To quote Derek Parfit 1987, p. 361: 'It may help to think about this question: how many of us could truly claim, 'Even if railways and motor cars had not been invented, I would still have been born?'.

of accumulative harm.[8] To introduce this notion, let me begin with a few examples:

The first example is of a person walking on a nice, green city lawn.[9] The enjoyment of the person is harmless in that the grass may be (infinitely) slightly damaged but will recover quickly. However, if many people were to follow, the exact threshold depending on the season, the amount of rainfall, and so forth, the lawn would be damaged. The overall result might be devastating to all: There would be no lawn left.

The second example considers the effect of exhaust gasses on our environment. The minor effect of exhaust emissions produced by one car may be considered negligible, yet the accumulation of exhaust fumes by multiple cars exceeds the threshold of harm (Feinberg 1984, p. 228) and causes substantial harm to our environment.

Finally, Andrew Kernohan portrays racism as an accumulative harm. Whereas one racist remark can be played out as marginal, the accumulation of racist remarks (and acts) is a serious harm:

> [S]omewhere between those minor cultural acts and those produced by millions of people with racist attitudes the threshold of harm is reached. (Kernohan 1998, p. 73)

Joel Feinberg explains accumulative harm as a harm inflicted by a collective, through the accumulation of multiple seemingly harmless acts (Feinberg 1984, p. 226). Especially with regard to individual perpetrators, the (eventual) harm is seemingly invisible, non-existent. As Kernohan writes:

> [I]n the case of accumulative harms, a harmed condition can arise which does not result from harmful conduct. (Feinberg 1984, p. 226)

The concept of accumulative harm has proved useful with regard to several different social phenomena and harms, such as the use of antibiotics in agriculture,[10] environmental issues (water and air pollution)[11] copyright infringement,[12] and money laundering.[13] Andrew Kernohan (1998) provides a thorough review and application of the concept to the phenomenon of cultural oppression. Although cultural oppression is often neither noticed nor noticeable, by both victims and perpetrators, Kernohan successfully demonstrates why cultural oppression is nevertheless morally harmful and state regulation is warranted. His aim is to

[8] van den Hoven 2000, p. 153 mentions Feinberg's notion of accumulative harm in 'The Internet and Varieties of Moral Wrongdoing.'

[9] This example was borrowed from Andrew Kernohan, who uses it in his book Liberalism, Equality, and Cultural Oppression to point to the differences in act- and rule- utilitarian thought in attending to this problem. See Kernohan 1998, p. 78.

[10] Cf., Anomaly 2009, pp. 423–435.

[11] Examples used by Feinberg 1984.

[12] Cf., Moohr 2003, pp. 731–784.

[13] Cf., Alldridge 2001, pp. 279–319.

justify state intervention with respect to people's conceptions of the good on grounds of the resulting diffuse and insidious accumulative harms.

My purpose for this chapter is to show that there is a similar potential harm in play in the context of IDM and e-government. It is what I call accumulative informational harm, harm resulting from the availability and assembly of multiple seemingly innocuous bits of information about one person. Parallel to the notion of accumulative harm as described above, the harm is hardly noticeable—let alone noticed—by looking at the separate elements which together make up for the potential harm in question; as metaphorically put in the illustrious 'cage' image of oppression by the feminist author Marilyn Frye (Kernohan 1998). The meaning of a cage is not grasped by studying its bars one by one, but by looking at the cage as a whole, i.e., at the accumulation of bars. The issue at stake thus concerns the potential harm created by the accumulation of multiple bits of sometimes seemingly innocent bits of (identity related) data.[14]

This brings us to a difference with Feinberg's notion of accumulative harm: Whereas Feinberg's notion of accumulative harm refers to the accumulation of acts, acts that may seem harmless but turn out harmful in retrospect of their collective sense, accumulative informational harm concerns the potential harm as a result of accumulating bits of principally harmless information. It turns out that in the example Feinberg provides, e.g., of air pollution and the example Kernohan gives of racism, the individual acts were harmful all along, only in a negligible sense. In the case of accumulative informational harm, the particular bits of information are usually not considered harmful on their own, it is rather the accumulation of data with a potential for causing harm. This can be compared with issues of overpopulation: There is nothing harmful about a squirrel in New York; only above a certain threshold, the clutter of squirrels proves to be a nuisance. And the same goes for the number of humans inhabiting this earth; there is principally nothing harmful about humans on this earth, however, overpopulation may lead to the depletion of natural resources (Colby 2009) and to a more rapid spreading of diseases (Simonetta 2009).[15]

Ethical theories, be it deontology, consequentialism, or utilitarianism, traditionally deal with issue—concerning readily identifiable victims and violations, i.e., with agents and (harmful) acts. In the case of accumulative informational harm however, as we have seen above, none of these elements are readily present or easily identifiable; neither victims nor perpetrators are known at all times, as are the acts leading up to the harm in question.

Even so, something here is amiss with regard to morality. Consider first that the ontology of traditional ethics is made up of identifiable agents. Conventionally ethical theory deals with the moral behavior of known actors: the identifiability of

[14] Interestingly, if we revisit what was said about free-riders in Sect. 5.1, we find that the issue of free-riders, understood as an example of accumulative harm, does not only fuel the identification of citizens and therefore the deployment of technologies such as IDM; in fact, IDM brings on a certain type of accumulative harm itself. Thanks to Sabine Roeser for pointing this out to me.

[15] For an appraisal of world population control policies, cf., Connelly 2008.

agents is a condition sine qua non.[16] For traditional ethics, the question is whether a particular agent's actions, affect or have affected the well-being of particular ethical beings, for better or for worse. By implication these agents (both victims and perpetrators) are identifiable. As discussed, this is not necessarily true for accumulative informational harms. In case of accumulative harm, the harm of a particular action may be negligible or (seemingly) non-existent. Although our purpose is to investigate a potential harm, neither perpetrators nor victims turn out to be identifiable. This conception of harm therefore falls under the category of (epistemologically) 'identity-independent' harms, which Page has framed as repudiating the necessity for particular ethical beings as objects of harm in assessing whether it is wrong to perform certain acts or adopt certain policies (Page 2006a, p. 138).

Moreover, traditional ethics deal with acts, with the implication of affecting the well-being of other (ethical) beings, for better or for worse. As pointed out by Walter Sinnott-Armstrong (2005, p. 289), our moral intuitions appear to have evolved to primarily handle cases with obvious implications. And Edward Page (2006a, p. 134) maintains that harm-based or identity-dependent reasoning is deeply ingrained in the ethics, law and common sense morality of most countries. Hence the moral vacuum with respect to cases where people are unaware of the long-term or unforeseen, provisionally invisible effects of their acts. In case of accumulative (informational) harm, the harm is not even necessarily associated with its preceding acts. As Kernohan puts it:

> [I]n the case of accumulative harms, a harmed condition can arise which does not result from harmful conduct. (Kernohan 1998, p. 72)

It is indeed questionable whether the 'acts' of accumulative (informational) harm can be identified as such. Although the collecting of information or decision-making, for example to set up a database, could be seen as acts, what is often truly at stake is the information generated as a by-product of a certain act. Consider the case of a search act on the Internet by means of using Google; the by-product of this act is information about one's search behavior, which is recorded and stored in a database. On the basis of this information individual- and group-profiles can be made, in both cases a matter of producing identity related data, i.e., information about a person's identity. This newly produced information in turn adds to the collection of multiple bits of information about a person potentially causing accumulative harm.

What follows from this discussion is that the elements of traditional ethics, i.e., the acts and agents, are not straightforwardly meaningful with respect to accumulative informational harm. If neither acts nor identifiable agents are self-evidently involved, the question remains as to what makes this phenomenon count as harm. To answer this question let us take a closer look at the concept and objects of harm.

---

[16] Another discipline where this can be clearly seen is game theory, which holds the basic assumption that players can be identified; there is no point in studying the behavior of unknown players.

Harm[17] is generally defined as a disvalue, a detriment, or a set-back to socially valuable interests. These interests can be of two kinds, i.e., welfare interests, and interests related to one's personal projects and goals. Feinberg then identifies three ways in which someone's interests may be impaired: (1) the circumstances may be modified making it difficult to satisfy (competing) interests; (2) the degree to which prudential interests are protectively diversified is reduced; or (3) one's welfare interests are directly impaired making it difficult for someone to pursue the second kind of (ulterior) interests. For accumulative informational harm in the context of IDM and e-government, this plays out for example as follows: (1) the opportunities for a citizen are modified on account of available information about him or her, e.g., profiles; (2) the range of options presented to the citizen to choose from (for different purposes) is limited as a result of available information or profiles; and (3) the pursuit of personal life choices is restrained as a result of the opportunities IDM provides for e-government.

Having addressed agents and acts as traditional elements of harm, and three possible ways in which harm can occur, what is left is a closer look at the objects of harm, i.e., who is affected. They are threefold: (1) individuals, (2) groups, and (3) culture.

Ad (1) The most straightforward object of harm, as discussed above in the context of traditional ethics, is the individual whom the information in IDM is about. In this case, what is under consideration is the way the individual's particular interests may be set back as a consequence of certain acts (either by a group or by another person).

Ad (2) A group can also be the object of harm. For example in case of air pollution or cultural oppression, all members of the group are equally harmed. In this case the group is harmed on the basis of the shared characteristics of the group. Even if this group was eventually to consist of only one person, for example if only one person was left to be affected by the harmful consequences of air pollution or cultural oppression, the object of harm patently remains the group for the equal harm it has previously caused for other members of the group.

Ad (3) The third object of harm includes the creation of a potentially harmful environment. As an illustration let us take the accumulation of weapons in the United States[18]: The mere presence of weapons is not harmful as such. Yet it does create a strong potential for harm, in other words it brings about a hostile environment. Culture as the object of harm is paramount for any government-related context. It raises the issue of what kind of environment we wish to pursue.

[17] According to Feinberg 1984, we must distinguish between a non-normative notion of harm as a setback to interests, and a normative notion of harm as a wrong. Yet in *Harm to Others* he offers a definition of harm as 'a wrongful set-back to other people's interests' in which he conflates both conceptions, i.e., setbacks to others' interests that are wrongs at the same time. For a critical discussion on this topic cf., Hurd 1994, pp. 210–213, and Stewart 2001, pp. 47–67.

[18] Thanks to Jeroen van den Hoven for this useful analogy.

What's more, this object of harm is instrumental to the first two. By means of a harmed culture, both individuals and groups are, or can be indirectly harmed.

Accumulative informational harm can affect all three objects of harm. First of all an individual could be harmed, e.g., as the result of incorrect identity related information stored in databases, or the improper treatment of a citizen on the basis of the incorrect application of a profile. Second, the technical hitches of a newly designed information infrastructure could (unintentionally) deprive certain groups or even all citizens of government services. Finally, the presence of elaborate digital files on citizens could contribute to a shift in power balance between citizens and government. The accessibility of personal information makes citizens more vulnerable, as is commonly known from (civil) wars such as in former Yugoslavia, World War II, and the Rwanda atrocities.

Priscilla Regan (1995) argues for privacy in connection with the latter object of harm concerning a change of environment. She argues that the problem with privacy is not that it harms individuals, nor members of a group by means of group characteristics; it is rather the 'privacy-infringing' culture of facile data exchange precipitated by modern technology that harms the environment. Hence she characterizes privacy as a public good, valuable not only to the individual but to society in general. She points out that what is at issue here is how we collectively choose to organize society.

The contribution of the availability of elaborate (digital) files on citizens to a shift in power balance between citizens and government has proven of concern to many thinkers. One of the influential scholars in this field, Oscar Gandy (1993), expresses discriminatory concerns as a result of the large-scale deployment of information technologies for the collecting, processing, and sharing of data about individuals. In his book 'The Panoptic Sort' he describes this mechanism as a 'technology of power,' exercising control over individuals through the sorting and self-sorting aspect of its functionalities. Gandy puts forward three worrisome developments with regard to the fast-pace maturing and associated integration of IDM and profiling technologies into everyday life: (1) the limitation and uneven distribution of available information, respectively provide options to choose from, (2) an increased instability in markets and politics due to the limited theoretical rationale of the systems deployed, (3) the destruction of trust and accountability within communities due to its totalitarian inclinations to include and conform individuals. According to Gandy, segmentation diminishes and eventually eradicates communication between different groups in society, thereby slowly undermining the public sphere and replacing it with multiple projected micro-experiences of a public life.

The discriminatory effects of profiling—and IDM technologies, I would add—are also underscored by David Lyon (2003), by what he calls 'surveillance technologies.' He warns for what can be seen as a new interpretation of the digital divide:

> To consider surveillance as social sorting is to focus on the social and economic categories and the computer codes by which personal data is organized with a view to influencing and managing people and populations … [I]n everyday life our life-chances are continually checked or enabled and our choices channeled using various means of surveillance. The

> so-called digital divide is not merely a matter of access to information. Information itself can be the means of creating divisions. (Lyon 2003, p. 2)

5.4 Regulating Invisible Harms

Accumulative informational harm results from the accumulation of multiple bits and pieces of information. This information is made available for example by the data subjects themselves, or through the administration, tracking and tracing of behavior, and characteristics of subjects, and by profiling. These informational processing techniques are closely connected with IDM and the opportunities such an informational infrastructure offers: the combining and linking of databases, the continuous updating of informational records, the structuring of massive amounts of available information by means of categorization, and so on. In short, the potential of accumulative informational harm comes with the very nature of implementing IDM (for any practice).

Having discussed accumulative informational harm as a risk of deploying IDM for e-government, what remains is how we deal with it. How do we anticipate possible negative side-effects of the widespread collection, mining, and use of data in IDM technologies, whilst taking advantage of its epistemic (and organizational) benefits? Is this particular trade-off surmountable?

Value-Conscious Design (VCD) refers to a number of approaches purporting to meet such trade-offs in design (Manders-Huits and Zimmer 2009, p. 38).[19] Would it be possible to avoid the phenomenon of accumulative informational harm by means of applying a VCD-approach, or is this particular kind of harm of a different order? Would it, for example, be possible to define thresholds for identity related information? Compare this with the working of a thermostat: it switches the energy supply off or on once the temperature reaches a certain critical limit. Would it be possible here to define such a limit?

After all, if we do not establish rules for dealing with our identity related data, our identities and individual biographies may be subject to the molding forces of macro-level institutional and cultural developments. Notably, this account is primarily an exploration of how we can responsibly take care of our social environment and the values within.

For this exploration I am sympathetic to the argument made by Priscilla Regan in Legislating Privacy that I have mentioned earlier, where she takes issue with privacy framed as an individual liberty (as opposed to a public good). She argues

[19] For frameworks included under this heading cf., 'Design for Values', Jean Camp, (n.d.), 'Values at Play', Flanagan et al. 2005; Flanagan et al. 2008, and Friedman et al. 2002.

that privacy is instrumental to a democratic and just society, and the establishment of trusting relationships in such society. According to Regan, viewing privacy as an individual right, elicits a misplaced trade-off—amongst other things—between privacy versus public security. It then seems as if there is a trade-off between individuals giving up their privacy for the common good of public security, e.g., in case of tax evasion or crime-fighting. However, as a public good privacy is valued for its instrumental worth for democracy and thereby applies to all citizens alike as opposed to the comparison of particular inequalities associated with an individualist approach.

The framing privacy as a public good rather than as a matter of individual rights, so I believe, corrects a misplaced trade-off between individual versus public values, such as privacy and public security in Regan's analysis. I think the key to resolving the trade-off between the potential benefits and harms of IDM for e-government as described in this chapter, lies in the prevention of accumulative informational harm, for example through the appreciation of privacy as instrumental to the design of our culture or social environment, while at the same time enjoying the epistemic and organizational gains of IDM for e-government.

Finally, what I propose as a starting point for the design and implementation of IDM technologies for e-government (and other purposes), and their regulation is a principle of minimalism: Record as little information as possible, for no longer as is strictly necessary, using a method or technology that is as robust as possible.[20] Though in practice this principle is in ongoing competition with economic and political forces such as control, security, and risk aversion, I argue that it nonetheless contributes to avoid the following pitfalls:

- The permanence of files and information they contain, irrespective, for example, of long-term developments in politics and policy. Information from records can be used and misused in the future for all sorts of reasons—think of the Second World War and how efficiently the Germans were able to do their detective work for demographic selection in the Netherlands, thanks to well-documented information on people's religious beliefs.
- The issue of ownership of information within large infrastructures and organizations. In complex systems it is not clear precisely who owns what information, who grants access, who manages the file(s), and who performs the necessary checks.

[20] For many purposes, a combination of minimum information and minimum technology is sufficient. A successful example is the project 'Verwijsindex Risicojongeren' (VIR). It is part of a Dutch national information system meant to provide insight to different care providers regarding each other's involvement concerning a particular adolescent. For more information see http://www.verwijsindex.nl/ (available only in Dutch). What makes it a success is that there is no centralized and permanent database; the technology in question only supports the collaboration between associated parties for a clearly confined purpose.

- The technical risks associated with large-scale information architectures, think of viruses, hacking, theft of information, carelessness.
- The inescapability of a person's profile: There is no such thing as a 'clean slate.' Although someone may have changed over the years, policy decisions and treatments may still be based on a former profile.
- The risks associated with incorrect information. The implementation of large-scale infrastructures reduce the risk of information not being available or being available in duplicate, but it increases the risk of the wrong information being available or information being incorrectly interpreted.
- The opportunities for malicious intent by manipulation on the basis of available data, e.g., identity fraud.[21]

5.5 Conclusion

In this chapter, I have discussed the overwhelmingly positive epistemic contribution of IDM for e-government. IDM adds to the epistemic power, speed, fecundity, efficiency, and reliability of e-government; moreover, it enhances organizational efficiency. On the other hand, the large-scale deployment of IDM for e-government also poses several risks, one of which involves accumulative informational harm. This potential harm is a result of the accumulation of multiple seemingly innocuous bits of information. Unlike traditional moral problems, neither victims nor perpetrators of this harm are readily identifiable. Nor are the preceding acts evidently harmful; the bits of information constitutive of the potential of accumulative informational harm are often by-products of other acts.

The challenge for thinking about values in design is to find out whether both the benefits of IDM for e-government can be kept, and harms prevented: Is this also possible in case of accumulative informational harm? One of the important considerations in this respect concerns the responsible design of our social environment. This is especially relevant in the context of e-government. An apposite starting point for the design of IDM for e-government is the principle of minimalism: It combines the ambitions and outspoken benefits of IDM whilst minimizing the amount of information needed in such design, so as to prevent reaching the threshold for accumulative informational harm.

References

Alldridge P (2001) The moral limits of the crime of money laundering. Buffalo Crim Law Rev 5(289):279–319

Anomaly J (2009) Harm to others: the social cost of antibiotics in agriculture. J Agric Environ Ethics 22(5):423–435

[21] For an account of harm on the basis of information cf., van den Hoven 2008, pp. 306–308.

Benantar M (2006) Access control systems: security, identity management and trust models. Springer, New York
Cohen A (2009) Compensation for historic injustices: completing the boxill and sher argument. Philos Public Aff 37(1):81–102
Colby K (2009) Current human population dangerous for planet. http://kevincolby.com/2009/04/01/current-human-population-dangerous-for-planet/. Accessed 15 October 2009
Connelly M (2008) Fatal misconception: the struggle to control world population. Belknap, Cambridge
Feinberg J (1984) The moral limits of the criminal law, Volume 1: harm to others. Oxford University Press, Oxford
Flanagan M, Howe D, Nissenbaum H (2005) Values at play: design tradeoffs in socially-oriented game design. Proceedings of CHI 2005, pp 751–760
Flanagan M, Howe D, Nissenbaum H (2008) Embodying values in technology: theory and practice. In: van den Hoven J, Weckert J (eds) Information technology and moral philosophy. Cambridge University Press, pp 322–353
Friedman B, Kahn P, Borning A (2002) Value sensitive design: theory and methods. Technical Report, University of Washington
Gandy O Jr (1993) The panoptic sort: a political economy of personal information. Westview Press, Boulder, CO
Hurd H (1994) What in the world is wrong? J Contemp Leg Issues 5(157):157–216
Kernohan A (1998) Liberalism, equality, and cultural oppression. Cambridge University Press, Cambridge
Laslett P, Fishkin J (eds) (1992) Justice between age groups and generations. Yale University Press, New Haven
Lyon D (ed) (2003) Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge, London
Manders-Huits N, Zimmer M (2009) Values and pragmatic action: the challenges of introducing ethical intelligence in technical design communities. Int Rev Inf Ethics 10:37–44
Moohr GS (2003) The Crime of copyright infringement: an inquiry based on morality, harm, and criminal theory. Boston Univ Law Rev 83(731):731–784
Page E (2006a) Climate change, justice, and future generations. Edward Elgar, Cheltenham
Page E (2006b) The non-identity problem. In: Page E (ed) Climate change, justice, and future generations. Edward Elgar, Cheltenham
Parfit D (1987) Reasons and persons. Clarendon Press, Oxford
Rawls J (1971) A theory of justice. Harvard University Press, Cambridge
Rawls J (1993) Political liberalism. Columbia University Press, Columbia
Regan P (1995) Legislating privacy: technology, social values, and public policy. University of North Carolina Press, Chapel Hill
Simonetta J (2009) Human overpopulation: causes, effects and solutions. Ezine Articles. http://www.ezinearticles.com/?Human-Overpopulation-Causes,-Effects-and-Solutions&id=1985200. Accessed 15 October 2009
Sinnott-Armstrong W (2005) It's not my fault: global warming and dividual obligations. In: Sinnott-Armstrong W, Howarth R (eds) Perspectives on climate change. JAI Press, Greenwich
Stewart H (2001) Harms, wrongs, and set-backs in Feinberg's moral limits of the criminal law. Buffalo Crim Law Rev 5(13):47–67
Thagard P (2001) Internet epistemology: contributions of new information technologies to scientific research. In: Crowley K, Schunn CD, Okada T (eds) designing for science: Implications from professional, instructional, and everyday science. Mawah, NJ, Erlbaum, pp 465–485. Also available in preprint (1997) at http://cogsci.uwaterloo.ca/Articles/Pages/Epistemology.html

van den Hoven J (2000) The internet and varieties of moral wrongdoing. In: Langford D (ed) Internet ethics. MacMillan Press, London, pp 127–157
van den Hoven J (2008) Information technology, privacy and the protection of personal data. In: Hoven J van den, Weckert J (eds) Information technology and moral philosophy. Cambridge University Press, Cambridge, pp 301–321

Part II
Policy Dimensions: Democracy

Chapter 6
The Single Point of Failure

Beth Simone Noveck

The world is full of amateurs: gifted amateurs, devoted amateurs. You can pick almost any group that has any kind of intrinsic interest in it, from dragonflies to pill bugs to orb-weaving spiders. Anybody can pick up information in interesting places, find new species or rediscover what was thought to be a vanished species, or some new biological fact about a species already known.

E.O. Wilson

Abbreviation

USPTO United States Patent and Trademark Office

Contents

6.1 The Closed Model of Decision-Making 78
6.2 New Technologies and Civic Life 81
6.3 Participatory Democratic Theory in the Age of Networks 86
6.3.1 The Failure of Direct Democracy 87
6.3.2 The Timidity of Deliberative Democracy 88
6.3.3 Distinguishing Deliberative and Collaborative Democracy 90
6.3.4 The Argument for an Open and Collaborative Democracy 92
6.3.5 Challenges for Collaborative Democracy 94
References 97

Contribution received in 2010.

This chapter is an excerpt from Noveck 2009.

B. S. Noveck (✉)
Institute for Information Law and Policy, New York Law School, New York, NY, USA
e-mail: bnoveck@nyls.edu

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*,
Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_6,

The patent system is just one example of how government institutions create single points of failure by concentrating decision-making power in the hands of the few, whether legislators in Congress, cabinet officials in the executive branch, or bureaucrats in agencies. Administrative practices are constructed around the belief that government professionals know best how to translate broad legislative mandates into specific regulatory decisions in the public interest. Governance, the theory goes, is best entrusted to a bureaucracy operating at one removed from the pressure of electoral politics and the biased influence of the public at large.

6.1 The Closed Model of Decision-Making

The rationale for this closed model of decision-making, as explained by such theorists as Max Weber and Walter Lippmann, is rooted in the assumptions of an earlier age. Although citizens may express personal opinions, they are thought to lack the ability to make informed decisions on complex policy matters. Moreover, democratic pessimists warn, government officials must be protected from the factionalized public, that Madison so feared in Federalist 10. To ward off this danger, centralized power is concentrated in the apolitical professional or, in Weber's words, 'the personally detached and strictly objective expert.'[1] Only government professionals possess the impartiality, expertise, resources, discipline, and time to make public decisions. Or so it is assumed. The assumption is not unjustified insofar as the technology has not been available before to organize participation easily. Participation in a representative democracy is largely confined to voting in elections, joining interest groups, and getting involved in local civic or political affairs.

Thus the patent examiner, like her counterparts throughout government, must act as an expert in fields far outside her ken. The process of determining which inventor deserves a patent demands that she analyze and synthesize scientific and technical information about cutting-edge areas of innovation, over which she has no real mastery. In any given subject area there are scientists, engineers, and lawyers with greater expertise, as well as laypersons with valuable insights, but the patent examiner has no access to them. In this, she is not alone. In a survey of environmental lawyers, for example, only 8% of respondents thought that the EPA has sufficient time to search the relevant science before making a decision about environmental policy, and only 6% believed that agencies employ adequate analysis in their decision-making.[2] The bureaucrat in Washington often lacks access to the right information or to the expertise necessary to make sense of a welter of available information. This can pose a challenge to good decision-making and to creativity in problem solving.

[1] Gerth and Wright Mills 1991.

[2] Ruhl and Salzman 2006.

The single point of failure results not just from a lack of time or resources, or technology. It goes much deeper than that. Simply put, professionals do not have a monopoly on information or expertise, as the social psychologist Philip Tetlock observes. In his award-winning book 'Expert Political Judgment,' Tetlock analyzes the predictions of professional political pundits against modest performance benchmarks. He finds 'few signs that expertise translates into greater ability to make either "well-calibrated" or "discriminating" forecasts.'[3] While smart people can explain, they often cannot predict and therefore make decisions based on spectacularly bad guesses.

Pacifists do not abandon Mahatma Gandhi's worldview just because of the sublime naïveté of his remark in 1940 that he did not consider Adolf Hitler to be as bad as 'frequently depicted' and that 'he seems to be gaining his victories without much bloodshed'; many environmentalists defend Paul Ehrlich despite his notoriously bad track record in the 1970s and the 1980s (he predicted massive food shortages just as new technologies were producing substantial surpluses); Republicans do not change their views about the economic competence of Democratic administrations just because Martin Feldstein predicted that the legacy of the Clinton 1993 budget would be a stagnation for the rest of the decade; social democrats do not overhaul their outlook just because Lester Thurow predicted that the 1990s would witness the ascendancy of the more compassionate capitalism of Europe and Japan, over the 'devil take the hindmost' American model.[4]

It turns out that professional status has much less bearing on the quality of information than might be assumed and that professionals—whether in politics or other domains—are notoriously unsuccessful at making accurate predictions. Or as Scott Page, the University of Michigan author of 'The Difference', pithily puts it: 'Diversity trumps ability'—this is a mathematical truth, not a feel-good mantra.[5]

Moreover, government or government-endorsed professionals are no more impervious to political influence than the impassioned public that bureaucrats are supposed to keep at arm's length. Often the scientists and outside experts, who are asked to give impartial advice to government are lobbyists passing by another name. The National Coal Council, made up, almost exclusively of coal industry representatives, sits on the Department of Energy's federal advisory committee on coal policy: the department has adopted 80% of the Coal Council's recommendations.[6] White House officials regularly replace experts on agency advisory panels with ideologues and political allies (or eliminate advisory councils altogether). An Environmental Working Group study finds that the seven EPA panels that evaluated proposed safe daily exposure levels to commercial chemicals in

[3] Tetlock 2005, p. 20.

[4] Ibid., p. 15.

[5] Page 2007.

[6] Sapien 2008.

2007, included 17 members who were employed by, or who received research funding from, companies with a financial stake in the outcome.[7]

In a published statement titled Restoring Scientific Integrity in Policy Making, over 60 preeminent scientists, including Nobel laureates and National Medal of Science recipients, lambasted George W. Bush's administration for having 'manipulated the process through which science enters into its decisions.'[8] In 2008, about 889 of nearly 1,600 EPA staff scientists reported that they had experienced political interference in their work over the last 5 years.[9] But if the Bush administration is among the more egregious violators of the presumed wall between politics and institutionalized expertise, its actions only go to show how easy it is for any executive to abuse his power, while claiming the mantle of expertise.

Taking a historical view, the journalist Chris Mooney, in his book, 'The Republican War on Science', persuasively explains that the marriage of big business to the religious right in the Reagan era has resulted in a systematic abuse of science in regulatory decision-making.[10] What began during World War II as an intimate relationship between science and politics—the flames of whose passion were fueled by the competitive jealousy of the cold war and the attentions of an intellectually inclined Kennedy administration—has now waned. The rise of conservatism spurred a movement to create alternative sources for scientific information. Hiding behind the skirt of science, antievolution and antiabortion politics create pressure to misrepresent science to serve political ends. At the same time, the fear by big businesses that scientific research might impel expensive environmental and consumer regulation, further contributes to a distortion of the use of science in policy making. Mooney readily acknowledges that the Left as well as the Right makes decisions on the basis of political value judgments, rather than facts. But whereas Democrats, he contends, sometimes conduct politics in spite of science, choosing to ignore the data in pursuit of a normative end, Republicans dress up politics as science and attempt to name such positions 'creation science' behind a veneer of scientific legitimacy.

The problem of relying solely on professionals is compounded by the practice of confidential decision-making. While federal government agencies are required by law to conduct meetings in the open (and many state governments have similar sunshine laws), this spirit is violated by regular backroom dealings with lobbyists.[11] Under the Bush administration, the attorney general changed the presumption of disclosure under Freedom of Information Act, requests away from the prevailing standard to make it more difficult for agencies to release information and allow agencies to defend decisions to withhold records 'unless they lack a

[7] Lunder and Houlihan 2008.

[8] Union of Concerned Scientists 2005.

[9] Union of Concerned Scientists 2008.

[10] Mooney 2005.

[11] Government in the Sunshine Act, P.L. 409, 94th Cong. 13 September 1976.

sound legal basis.'[12] President Obama changed it back. It is not surprising that the American people perceive government to be taking place behind closed doors (three-quarters of American adults surveyed in 2008 view the federal government as secretive, an increase from 62% in 2006).[13] Massive financial bailout measures taken late in 2008 met with concerns that these troubled asset relief programs lacked transparency or monitoring. There have been myriad instances of information being deliberately hidden.

The Bush administration threatened to shut down the award-winning economic indicators website, which combines data like GDP, net imports and exports, and retail sales to make it convenient for viewers to assess the state of the economy.[14] The administration also announced it would no longer produce the Census Bureau's Survey of Income and Program Participation, which identifies which programs best assist low-income families, and stop publishing its report on international terrorism, making it more difficult for citizens to find important and useful news.[15] The Bush administration has taken down reports about mass layoffs and, by executive order, limited the publication of presidential records.[16] Until 1999, the USPTO did not publish patent applications until they were granted.[17] Even today, the office is circumspect about Internet research to avoid compromising the privacy and confidentiality of the decision-making process.[18] The less those outside the government know about its activities, self-evidently, the greater the need to rely on internal experts. When the public cannot see how decisions are arrived at, it cannot identify problems and criticize mistakes. Accountability declines, and so does government effectiveness.

6.2 New Technologies and Civic Life

Technology enables collective action in civil society and helps some people to route around the logjam created by the single point of failure. Countless civic groups already use new communication and information-sharing tools to promote political action, operate an opposition movement, or mobilize community

[12] Ashcroft 2001.

[13] More People See Federal Government as Secretive; Nearly All Want to Know Where Candidates Stand on Transparency 2008; Gup 2007.

[14] Terkel 2008.

[15] Kiel 2007.

[16] Ibid.

[17] American Inventors Protection Act, P.L. 113, 106th Cong. 29 November 1999.

[18] U.S. Patent and Trademark Office, Manual of Patent Examining Procedures, sec. 904.02(c) (8th edn. 2001) ('This policy also applies to use of the Internet as a communications medium for connecting to commercial database providers'); U.S. Patent and Trademark Office, 'Patent Internet Usage Policy', 64 Federal Register (21 June 1999) ('If security and confidentiality cannot be attained for a specific use, transaction, or activity, then that specific use, transaction, or activity shall NOT be undertaken/conducted'), p. 33,060.

activism. Collaborative governance needs to be distinguished from this kind of civic action that is independent of government—Change.org instead of Change.gov.

The Carrotmob project (http://carrotmob.org) in San Francisco uses the 'carrot' of consumer buying power to encourage small businesses to help the environment. Web-based tools are used to organize a consumer 'flashmob,' which channels business to stores, that commit to environmental improvements. Carrotmob organizer Brent Schulkin asked local businesses how much they would be willing to invest in environmental improvements if the group he convened were to organize a buying spree directed toward that business. The result for the winning bodega in San Francisco's Mission District: more than triple the sales of an average Saturday, lots of free advertising, oodles of community goodwill, and a scheme to pay for improvements that, in turn, will save the business money over the long run.

Similarly, Obama Works (http://www.whyobamaworks.org), a corps of self-organizing citizen volunteers with no connection to Barack Obama's presidential campaign, used Internet technologies to organize neighborhood cleanups not only on a local scale but also on a national scale. Tech for Obama (http://www.techforobama.com) similarly galvanized support for the campaign within the techie community. Supporters, independent of the campaign, even went so far as to create 'campaign offices' to recruit volunteers and organize voters. The largest one, in Silicon Valley, California, started on 15 December 2007.[19] Its Neighborhood Teams project geocoded the records of 1.5 million voters and used them to help over 40,000 neighbors find each other and volunteer in support of Obama. They produced and sent daily email newsletters to 5,000 people. Its 35-person technology team built its own tools to overcome inefficiencies in the organizing process. For its part, the official Obama campaign organized a summer program for Obama fellows (students and recent graduates who were recruited online) to come together and spend 6 weeks learning basic organizing skills from grassroots leaders. Senator Obama also spoke out publicly about creating a grassroots civic structure that could survive the campaign and continue to work on community issues after the election. In addition to meeting face to face, these volunteers used the Internet to form groups, organize, and bring about social change.

Both Carrotmob and the activities swirling about the Obama campaign are vivid examples of the use of new media technologies to convene and organize groups of people who, working together, can be more effective than any individual acting alone. Other examples include powerful online netroots organizations and blogs, ranging from MoveOn.org on the left, to Red State at the other end of the political spectrum.

Civic groups also take advantage of new technologies to shine the light of greater transparency on government from afar. These third-party brokers of transparency are helping to do what government is not doing enough for itself.

[19] Silicon Valley for Obama, http://www.sv4obama.com

The Cato Institute's Jim Harper launched the WashingtonWatch (http://www.washingtonwatch.com) program to track bills in Congress and estimate their cost or savings, if implemented into law. The Center for Responsive Politics started OpenSecrets (http://www.opensecrets.org); and the New York Gallery Eyebeam launched FundRace (http://fundrace.huffingtonpost.com) (now part of the Huffington Post blog) to make the Federal Election Commission's databases easier to understand and search. PublicMarkup.org (http://www.publicmarkup.org) used collaborative editing software, known as a wiki, to mark up the Transparency in Government Act of 2008 and the various economic stabilization and bailout proposals floated during the economic crisis in the fall of that year.[20] MAPLight.org (http://maplight.org) shines the light of transparency on money politics by illuminating who contributed to which politician and how he or she subsequently voted.

But while online communities to date may have enabled people to click together instead of bowling alone, they are not yet producing changes in the way government institutions obtain and use information. These purely civic programs are disconnected from the practices and priorities of government. They may circle around political themes and issues but are not tied into institutional processes. They are, therefore, limited in what they can accomplish. A few pioneering programs, such as Connecticut's City Scan program, suggest forms that such change might take, were we to redesign, rather than try to route around the workings of government.[21] Launched in the mid-1990s by the Connecticut Policy and Economic Council, CityScan helped city governments in Bridgeport and other municipalities, collaborate with local communities to rescue derelict land-use sites. The organization secured a promise from each city to assist with the cleanup of a given number of parcels. Senior citizens and young people used first-generation digital cameras and hand-held devices to photograph and track the progress of the work in their own communities. They mapped conditions on a website. The community groups communicated local information about land use that the government would not otherwise have had. They worked alongside the government while holding it accountable.

The government, in turn, worked with the CityScan teams, taking action based on their input and thereby giving relevance and impetus to these volunteer efforts. Technology helped both sides to organize the collaboration and to visualize its success. But the crux of CityScan was not the tools. The practices that CityScan evolved for robust collaboration between groups of citizens and local government, are what differentiated this work from that of most civic action.

Collaboration and collective action, of course, are not new. Since the early nineteenth century, members of the August Athenaeum Club on Pall Mall in London have penned questions in a shared book, which was left in the club's

[20] See also Miller 2008.

[21] Connecticut Policy and Economic Council, http://www.city-scan.org, Accessed October 2008.

leather-chaired drawing room for other members—including Dickens and Thackeray—to answer.[22] The book is still there.

As Stephen Kosslyn, chair of the Harvard Department of Psychology, explains, working together allows people to utilize many different tools. He says that, because we 'simply do not have enough genes to program the brain fully in advance,' we must extend our own intelligence with what he terms social prosthetic systems.[23] At the most basic level, we need to pool our diverse knowledge and skills. Even institutions need prosthetic extensions to make themselves smarter and more effective.

Virtually all activities of public life, including activism and organizing, depend on the work of teams. Until recently, however, most teams have relied heavily on physical proximity.

In the pre-Internet era, when working at a distance was not possible to the same extent (I had to be near you to join you), participation would have demanded a far greater time commitment to a cause. In the decade leading up to the American Revolution, the colonies organized Committees of Correspondence to communicate their practices of self-governance and fortify their opposition to the British.[24] Through the exchange of ideas about successful ways of working, they coordinated, decentralized efforts at resistance across a distance. But they were committed to this all-important cause. Anything less and one would still have had to attend meetings to accomplish shared goals or alternatively pay dues to an organization, to work on one's behalf. The ability now to use new technology to organize shared work, makes it possible to work in groups across distance and institutional boundaries. Technology can reinforce the sense of working as a group by recreating some of the conditions of face-to-face work environments that build trust and belonging. The ability to organize collective activity puts more power in the hands of individuals by making it possible for people to self-organize and form teams around a boundless variety of goals, interests, and skill sets. And technology can support the formation of larger and more complex teams than previously imaginable.

Not surprisingly, the software community has been in the forefront of efforts to tap these benefits. Harvey Anderson, general counsel of the Mozilla Foundation, which makes the Firefox browser, says of the Mozilla community of volunteer programmers: 'Many is better than one.' He echoes a common refrain among those who work on open source governance: 'Whenever we confront a problem, we have to ask ourselves: How do I parse and distribute the problem? How might we build feedback loops that incorporate more people?'[25]

The volunteer efforts extend the capacity of the full-time staff at Mozilla. By asking a community to help fix bugs in the software and rewrite the code, the organization begins to rely more and more on its community of volunteers, most of

[22] Cowell 1975.

[23] Kosslyn 2006, Wooley et al. 2007.

[24] Collins 1901.

[25] Anderson 2008a.

whom are not full time and most of whom may not even be known to the central project leadership. Instead, by articulating a set of common goals, the Mozilla Foundation helps disparate groups of people organize themselves and perform practical, concrete tasks toward a shared end.[26] What begins as a process of information gathering, builds steam and ends up creating a culture of engagement. Whereas the Mozilla organization makes the final decision about which software version to release, and when, the centralized organization cannot make these decisions without the help of the community of volunteers upon whom it relies to do the work. As the community comes to be more involved, actual decision-making becomes a more amorphous concept, and control becomes dispersed. Everyone in the network has an influence.

Similarly, when a policy problem is divided into smaller parts, so that it can be distributed and worked on by collaborative teams, the drive toward openness and innovation begins. This openness may help government do its job better by bringing better information to the institution. But it can also introduce the institutional priorities to more people so that competition for solutions can emerge. Impelled by government mandate, the private sector and civil society might suggest their own solutions, evolving more robust public–private approaches, which may produce greater legitimacy than government currently enjoys. It may also help to solve complex economic and social problems faster, and more efficiently.

New networking technologies, such as those embodied in Peer-to-Patent (http://www.peertopatent.org), provide an opportunity to rethink the closed practices by which agencies gather information and make decisions. In 2007, the US Congress mandated, and the president signed, a complete changeover by 2014 from incandescent bulbs to new, energy-efficient but mercury-containing lightbulbs. Congress instructed the EPA to implement the law into regulations. The agency, however, did not yet have a plan for disposing of the 300 million new mercury-containing bulbs sold in the United States in 2007—a number that will only increase as the mandate approaches.[27] The EPA could have solved this problem at little additional cost by setting up a simple online platform to involve a network of concerned citizens and organizations in identifying both the challenges raised by the new law and possible solutions—a lightbulb clearinghouse. Private sector companies might have stepped up to offer mercury reclamation programs sooner; foundations might have funded prizes to social entrepreneurs who devised effective solutions; interest groups might have run competitions among their members for effective recycling practices; scientists could have pointed out that

[26] Baker M, Mozilla Foundation chairman of the board 2008.

[27] 'Energy Bill Bans Incandescent Lightbulbs.' For more on mercury in lightbulbs, see the EPA website, http://www.epa.gov/epawaste/hazard/wastetypes/universal/lamps/index.htm. For more on the congressional mandate, see Wald 2007.

they were working on the creation of a 'nanoselenium' cloth to clean up mercury spills.[28] Creating new channels of communication would not only inform and improve information gathering, but it could also lead to improved decision-making and greater citizen involvement.

Policy makers have been slow to seize these opportunities. Innovation is not emanating from Washington; instead, the practices of government are increasingly disconnected from technological innovation and the opportunity to realize greater citizen participation—and therefore more expert information—in government. At the very least, this means that government institutions are not working as well as they might, producing declining rates of trust in government. (In 2008 the approval rating of both Congress and the president declined below 30% and, in some polls, even below 10%.)[29] At the very worst, there is a crisis of legitimacy. Clearly, relying on a small number of institutional players to make important decisions is not the only or the best way to confront complex social problems.

One explanation for this government failure lies in the unfamiliarity with technology displayed by many policy makers, including those responsible for its regulation. In the debate over net neutrality, then Senator Ted Stevens of Alaska, vice chair of the Senate Subcommittee on Science and Innovation, infamously referred to the Internet as 'a series of tubes.[30] While tubes could arguably be a reasonable metaphor, history has not been kind to Senator Stevens, whose literal remark has now become iconic (it has its own Wikipedia entry) of Washington's ignorance of technology. But lack of technical knowledge is not the only cause of the government's slowness to capitalize on the promise of networked, online groups. An even more fundamental explanation lies in the outdated theory of participatory democracy, that drives the design of government institutions.

6.3 Participatory Democratic Theory in the Age of Networks

After the advent of the World Wide Web, many anticipated that the Internet would revolutionize government, enabling an increase in political participation: an e-democracy as well as an e-commerce revolution. Pundits heralded a new Periclean Golden Age and celebrated the civic opportunities of the new communications and

[28] Fountain 2008.

[29] Newport 2008; 'Congressional Approval Falls to Single Digits for First Time Ever', 8 July 2008. http://www.rasmussenreports.com/public_content/politics/mood_of_america/congressional_performance

[30] 'Series of Tubes', http://en.wikipedia.org/wiki/Series_of_tubes. Also see the Series of Tubes weblog, http://www.seriesoftubes.net (Accessed October 2008). The remark also spawned a graphic, 'Series of Tubes as a Tube-map', http://www.boingboing.net/2007/07/20/series-of-tubes-as-a.html

information technologies.[31] The deliberative ideal of people with diverse backgrounds and differing viewpoints debating and even voting on public issues, was about to become a reality. It did not happen.[32]

6.3.1 The Failure of Direct Democracy

Proponents of direct democracy (sometimes called pure democracy) hoped that the Internet would promote participation unmediated by representative politics by allowing citizens to express themselves through voting (referenda, initiatives, recalls) more often on a wider range of issues.[33] Direct democrats argue for the use of technology to bolster such forms of direct participation as the initiative, and referendum as a way to speed up the pace of governance.

During his presidential bid, Ross Perot celebrated the direct democratic ideal and advocated that the president communicate directly with the American public via new media and encourage the public to vote regularly and directly from home on issues.[34] Auburn University houses a center dedicated to tele-democracy—large-scale, Internet-enabled, direct democracy.[35] Aficionados of proxy voting like the idea of using the web to allocate one's votes to a trusted interest group of one's choosing, to render direct democratic voting better informed and more practical to administer.[36] A now-defunct Swedish company pioneered online proxy voting in the political arena, a practice in common use in the corporate sector.[37]

But security and reliability problems have plagued the rollout of both electronic, kiosk-based, voting, and Internet-based vote-from-home technologies in the United States. Annual political elections are hard enough to run without introducing yet more possibilities for voter fraud and abuse. Instead, new services, such as Smartvote.ch from Switzerland, use the Internet to inform voting at the polling booth. Smartvote allows the user to plug in opinions in response to questions. The software then tabulates which candidate or proposal is closest to the user's own views. Countless informational websites have sprung up around the electoral process, whether it is the Washington Post's subscription service to inform the reader every time her elected official casts a vote, or one of myriad webcasts of

---

[31] See, for example, Chadwick 2006.

[32] Noveck 2005.

[33] Cronin 2006.

[34] Krauthammer 1992, p. 84.

[35] Center for Tele-Democracy, https://fp.auburn.edu/tann/. See also Direct Democracy League, http://www.ddleague-usa.net

[36] Volokh 2001.

[37] The company was Vivarto Inc., founded by Mikael Nordfors. Its website is, http://www.vivarto.com(online)

online legislative coverage designed to inform and render the political process more accountable by virtue of its being transparent.[38]

But the notion of widespread, push-button democracy in whatever form, does little to address how to institutionalize complex decisions in particular cases. It is no wonder that the vision of participation by direct democratic voting has not taken off.

6.3.2 The Timidity of Deliberative Democracy

Deliberative democracy has been the dominant view of participation in contemporary political theory. At its center is the Habermasian notion that the reasoned exchange of discourse by diverse individuals, representative of the public at large, produces a more robust political culture and a healthier democracy.[39] It has almost become a commonplace that people of diverse viewpoints should talk to one another town-hall-style in public (this despite the fact that some recent empirical research even suggests that talking to people of differing viewpoints correlates to reduced participation in community life).[40] It is a normative, democratic ideal unto itself and a means to the end of enhancing legitimacy in governance.

With the reduction in the cost of communications since the Internet, the hope had been that new information technologies would result in more widespread deliberation. Early e-democracy thinkers were optimistic that new technology could promote open discourse, equal participation, reasoned discussion, and the inclusion of diverse viewpoints. By allowing diverse participants to come together regardless of the boundaries of geography and time, the Internet could help overcome the hurdle of groupthink—a state in which like-minded people fail to consider alternatives adequately and fall prey to their own ideology.[41] Like direct democrats, advocates of deliberative democracy have also been disappointed. While social-scientific experiments in deliberation proliferate, there emerge deliberative theory founders on the practical reality of present-day political decision-making. In practice, such conversations have been difficult to achieve, especially on a large scale.[42]

The weakness of the deliberative approach is not that it reaches too far (as direct democracy may), but that it does not reach far enough. By making talk, the centerpiece of its normative aspirations, deliberative democracy's proponents assume that people are generally powerless and incapable of doing more than

---

[38] 'The U.S. Congress Votes Database', http://projects.washingtonpost.com/congress/rss/; Meskell 2007.

[39] Ackerman and Fishkin 2004, Fishkin 1991, Bohman 1996.

[40] Mutz 2006.

[41] Sunstein 2003, p. 118.

[42] Macintosh and Coleman 2003.

talking with neighbors to develop opinions or criticizing government to keep it honest. In theory, convening people of diverse viewpoints can have a beneficial impact on policy—assuming that the political system is structured to translate those viewpoints into meaningful participation in decision-making.[43] But in practice, civic talk is largely disconnected from power. It does not take account of the fact that in a Web 2.0 world, ordinary people can collaborate with one another to do extraordinary things.

The anthropology of deliberative participation leads to practices designed to present the finished work of institutional professionals, spark public opinion in response, and keep peace among neighbors engaged in civic discourse. The goal is not to improve decision-making, for 'there is no one best outcome; instead, there is a respectful communicative process.'[44] The desire for civilized discussion and dispute resolution lead to a requirement of demographically balanced representation in the conversation. This may ensure inclusion of all affected interests, but does not, as Alexander Meiklejohn said, necessarily result in an airing of all ideas worth hearing.[45] Deliberative democracy relegates the role of citizens to discussion only indirectly related to decision-making and action. The reality of deliberation is that it is toothless. Perhaps it is, as Shaw once said: the single biggest problem in communication is the illusion that it has taken place.

In 2002, for example, the Civic Alliance to Rebuild Downtown New York (with the help of AmericaSpeaks, a civic group that organizes public deliberation, and the sponsorship of the Lower Manhattan Development Corporation) convened Listening to the City, a demographically representative deliberation exercise that brought 4,500 New Yorkers together in person and 800 online to talk about the first set of designs for the World Trade Center site.[46] After hearing a presentation of the proposed plans, the group was highly critical. The high-profile, public nature of the event attracted a front-page story in the New York Times. It directly led to officials scuttling the plans and initiating a second round of designs.

The people power, as the populist historian Howard Zinn might say, of a large number of people massing in physical space created political pressure.[47] But people were neither expected nor invited to offer advice and expertise to inform the new plans. In this carefully orchestrated deliberation, they did not have an opportunity to get involved in the cleanup or to identify problems or solutions to the mounting environmental and economic development challenges in the area. The problem was not presented in ways that could have led to private sector assistance, either in the government's effort or as an adjunct to it. Nothing about the weekend changed or improved the way government works. Arguably, the Lower Manhattan Development Corporation used the Listening to the City

[43] Shane 2004.

[44] Czapanskiy and Manjoo 2008.

[45] Meiklejohn 1960.

[46] Wyatt and Bagli 2002, p. A1.

[47] See, for example Zinn 2007.

exercise to appear responsive to citizens' concerns while obscuring the real power politics at play, ultimately depriving New Yorkers of the chance to participate, rather than simply react.[48]

The political sociologist Michael Schudson writes about the "monitorial citizen," who is too busy to play an active role in government.[49] While it is important and useful that government is responsive to the watchful citizen, this passive vision does not recognize the full potential of ordinary people to share expert information and effort with government. Among members of the public are scientists, engineers, doctors, lawyers, students, teachers, and nonprofessionals with a wide range of experience and enthusiasm who can contribute to an understanding of energy independence by submitting data. Others can analyze information given to them about endangered species or participate in the drafting of policies about transportation. There are expert conferences daily, where instead of presenting disconnected academic papers, these great minds might also be enlisted to solve pressing social problems. These potential resources for public decision-making are largely going to waste.

6.3.3 Distinguishing Deliberative and Collaborative Democracy

There is a difference within participatory democracy between the two related, but distinct notions of deliberation and collaboration. Deliberation focuses on citizens discussing their views and opinions about what the state should and should not do. The ability for people to talk across a distance facilitates the public exchange of reasoned talk. But deliberative polls, neighborhood assemblies, consensus councils, citizen panels, and other conversation-centered experiments, whether online or offline, have not translated into improvements in decision-making practices. The underlying Internet and telecommunications infrastructure is essential to conversing across a distance, but the Internet by itself is not the 'killer app.' If it were, the history of citizen participation in government institutions, which I describe in Chap. 6 of Noveck (2009), would already look very different.

While both deliberation and collaboration may be group-based, deliberative democracy suffers from a lack of imagination in that it fails to acknowledge the importance of connecting diverse skills, as well as diverse viewpoints, to public policy. Whereas diverse viewpoints might make for a more lively conversation, diverse skills are essential to collaboration.

Deliberation measures the quality of democracy on the basis of the procedural uniformity and equality of inputs. Collaboration shifts the focus to the effectiveness of decision-making and outputs.

---

[48] Sorkin 2003, pp. 57–61.

[49] Schudson 1998.

Deliberation requires an agenda for orderly discussion. Collaboration requires breaking down a problem into component parts that can be parceled out and assigned to members of the public and officials.

Deliberation either debates problems on an abstract level before the implementation of the solution or discusses the solution after it has already been decided upon. Collaboration occurs throughout the decision-making process. It creates a multiplicity of opportunities and outlets for engagement to strengthen a culture of participation and the quality of decision-making in government itself.

Deliberation is focused on opinion formation and the general will (or sometimes on achieving consensus). Consensus is desirable as an end unto itself.[50] Collaboration is a means to an end. Hence the emphasis is not on participation for its own sake but on inviting experts, loosely defined as those with expertise about a problem, to engage in information gathering, information evaluation and measurement, and the development of specific solutions for implementation.

Deliberation focuses on self-expression. Collaboration focuses on participation. To conflate deliberative democracy with participatory democracy, is to circumscribe participation by boundaries that technology has already razed. In fact, the distinctions between deliberation and collaboration become even more pronounced in the online environment, whose characteristics are increasingly making collaboration easier.[51] New technologies make it possible to join ever more groups and teams. Such familiar websites as Wikipedia, Facebook, and even video games like World of Warcraft inculcate the practices of shared group work, be it writing encyclopedia entries or slaying monsters, at a distance.

New technology is also making it possible to divvy up tasks among a group. 'Digg-style' tools for submitting and rating the quality of others' submissions have become commonplace ways to sort large quantities of information. Finally, the digital environment offers new ways to engage in the public exchange of reason. With new tools, people can 'speak' through shared maps and diagrams, rather than meetings. Competing proposals, using computer-driven algorithms, and prediction markets, can evolve. Policy simulations using graphic technology can be created. Social networking tools enable collaborative making, doing, crafting, and creating. Yet most of the work at the intersection of technology and democracy has focused on how to create demographically representative conversations.[52] The focus is on deliberation, not collaboration; on talk instead of action; on information, not decision-making.

---

[50] There are numerous proponents of this 'strong' theory of civic engagement: Barber 1984, Sclove 1996, Skocpol and Fiorina 1999.

[51] Balkin 2004.

[52] The ideal type of citizens' group is one that is 'composed of representatives of all strata of its community; it would be unbiased, courteous, well-organized, adequately financed, articulate.' Guimary 1975, p. 148.

6.3.4 The Argument for an Open and Collaborative Democracy

The case for an open and collaborative vision of democratic theory is bolstered by three arguments: collaboration as a distinct form of democratic participation, visual deliberation, and egalitarian self-selection.

First, collaboration is a crucial but not well understood claim of democratic practice. There is a belief that the public does not possess as much expertise as people in government. Furthermore, the technology has not previously existed to make collaboration possible on a large scale. These spurious assumptions have produced an anemic conception of participatory democracy. Participation has generally referred to once-a-year voting or to community deliberation, in which neighbors engage in civil dialog and public opinion formation on a small scale. New social and visual technologies (sometimes referred to as Web 2.0) are demonstrating that people are knowledgeable about everything from cancer to software and that, when given the opportunity to come together on a network and in groups, they can be effective at solving problems (not only deliberating about them). We must therefore distinguish between deliberation and collaboration as forms of participatory practice, exploring many examples of ordinary people joining together to do extraordinary things coordinated via the Internet. Peer-to-Patent is a paradigmatic case of database programmers and wind-farming experts working with patent examining professionals to make a better decision.

Second, the medium matters. To enable collaboration at scale, requires designing the practices to make participation manageable and useful and then enabling those practices by means of technology. While the forms of participation will differ when information gathering or priority setting or data analysis are required, the technology should always be designed to reflect the work of the group, back to itself so that people know which role they can assume and which tasks to accomplish. This second insight is what I term visual deliberation. In traditional deliberative exercises, strict procedures for who can talk, govern the public conversation. But collaboration depends, instead, on having tools that convey the structure and rules of any given collaborative practice. This kind of social mirroring can be communicated through software. Peer-to-Patent uses visualizations to communicate the workflow by which information goes from the government institution to the public and back again. The website helps to convey what it means to review a patent application. It exploits rating and reputation techniques that help each group work together as a group, even across a distance. Hence, designing new democratic institutions also depends on designing the appropriate collaborative practices and embedding that design in software.

Third, collaboration is a form of democratic participation that is egalitarian—but egalitarian in a different way than the traditional understanding of the term. Typically, mass participation like voting is thought of as being quite democratic because everyone can participate in the same way. By contrast, Peer-to-Patent is not a mass participation. It demands highly technical expertise. Successful participation depends upon the participant's interest in and knowledge of patents.

If Peer-to-Patent was the only example of collaborative participation, it would not be egalitarian. But Peer-to-Patent multiplied by a thousand would be more institutionally diverse and complex. If the patent expert and the doctor, and the teacher each have a vehicle for engagement, contexts would be created in which they each uniquely possess expertise and derive meaning.

In other words, people do not have to participate in the same exercise. One person may want to work on Peer-to-Patent, another may want to get involved in health care debates. One person may want to work on energy policy, another may want to organize a corps of energy "scouts" to go door-to-door and help neighbors evaluate their energy usage. The ability to self-select to participate in the arena of one's choosing is what makes collaborative democracy egalitarian. A person may be an expert on wetlands because she possesses professional credentialing. Another person may be an expert on wetlands because she lives near one. Perhaps it is a level of know-how or the enthusiasm to commit more time, that generates status in other domains. For every project, there is a different kind of expertise, which could be sought. Experts will flock to those opportunities that exploit their intelligence. In this choice lies the equality of opportunity.

What does open and collaborative democracy look like in practice? In the old way of working, the bureaucrat might decide to repair a bridge in response to an opinion poll or vote that randomly obtains feedback. Or the bureaucrat might publish a fully developed plan to repair the bridge, ostensibly soliciting comment in response to a notice of proposed regulation, attracting participation by formal interest groups and lobbyists, but not ordinary citizens, who can never hope to match the power and influence of corporate interests. Community groups might use the web to lobby for bridge repair but with no greater opportunity to get involved in detailed decisions. The government or a nongovernment organization (NGO) might organize a face-to-face deliberative discussion about the bridge and hope to use the event to trigger a newspaper article that will influence the decision. A similar online discussion may or may not attract attention.

Under a collaborative strategy, the bureaucrat establishes the process, then frames and asks the questions that will get targeted information from bridge users (the truck driver, the commuter), from an engineer, and from the informed enthusiast. The public can contribute evidence and data to help inform specific decisions, analyze data once gathered, and share in the work of editing, drafting, and implementing policies. Alternatively, if officials articulate the priority of bridge safety, they might spur private sector businesses, nonprofits, and individuals to develop their own strategies, such as organizing a volunteer corps of bridge safety inspectors who log their work on a shared website. Citizens are no longer talking about the process: they are the process.

The future of public institutions demands that we create a collaborative ecosystem with numerous opportunities for experts (loosely defined as those with expertise about a problem) to engage. There is a Plum Book, which lists government jobs, and there is a Prune Book, which lists the toughest management positions. The pluot is supposed to be the sweetest variety of plum (or plum plus apricot). Yet there is no 'Pluot Book' cataloging opportunities for part-time

participation in government! When participatory democracy is defined to include diverse strategies for collaboration, when these thousands of opportunities to self-select come to light, a Pluot Book may well be needed.

6.3.5 Challenges for Collaborative Democracy

Critics might suggest that there already exists an architecture of participation, involving a wide array of actors in policy-making processes. Corporations participate through lobbyists and notice-and-comment rule-making. Nongovernmental organizations, too, funnel information to government through think tanks, white papers, and publications. Interest groups lobby and enlist their members to respond—usually through postcards and email—in rulemaking and legislative policy making. Scientists and others participate in deliberative, small-group, federal advisory committees that give advice to officials. With more public deliberation exercises, when they take place, help to generate opinion formation.

What is lacking, though, are effective ways for government to be responsive to the public, as opposed to corporate interests, large stakeholders, and interest groups. These citizen participation strategies suffer from the problem of 'capture'—excessive political influence. Nominees are often subjected to ideological litmus tests. Lobbyists use their ability to participate to stall, rather than inform the regulatory process. The use of notice-and-comment periods (in response to agency-proposed rule-making), which solicit individual participation, is typically late in the process, when policies are all but finalized. And people are too busy anyway to do the work of professionals in government.

What will prevent new, networked publics from becoming as entrenched as the lobbying culture that has produced the failures of current politics is that collaborative democracy seeks to proliferate many smaller opportunities for openness. The EPA does not need 100,000 people to work on the issue of asbestos or mercury. While some issues attract a huge number of people, obscure (yet important) decisions are made every day in government that could be made better if technology were used to open participation and oversight to a few dozen experts and enthusiasts—those that blogger Andy Oram calls the microelite: the 5 or 10 or 100 people who understand a discrete question and who are passionate about getting involved in a particular way.[53] Collaborative democracy is about making it easier for such people to find the areas where they want to work and contribute.

Some will counter that more active involvement in government by self-selecting private citizens would only increase the risk of corruption. Their fear is that opening up channels of participation would create a whole new class of online lobbyists and campaigns that participate to serve their own financial interests. True perhaps. But if the practices of twenty-first-century government were designed to

[53] Oram 2007.

split up tasks into many small fact-gathering and decision-making exercises, technology would diversify against that risk. It is harder to corrupt a system with many parts. This approach would also make it easier for busy people to participate. And if government decisions were designed to be made in groups, group members would keep each other honest and blow the whistle if corruption occurs.

The primary challenge when engaging in deliberation is to avoid capture and corruption by those who speak with the most influence. In a collaborative governance environment, the greatest challenge is one of design: organizing the work most effectively to tap outside expertise. The bureaucrats who design the collaborative processes might be tempted to set them up in such a way as to promote participation by particular vested interests over others. But open processes that enable people to evaluate one another's participation help to preclude the risks. At the very least, technology makes it possible to organize decision-making in ways that might overcome abuses familiar from the offline world. If governance is thought of as a granular and focused set of practices, ways can be designed to delegate greater power to citizens to gather facts, spend money, and participate in decision-making.

Giving ordinary people—as distinct from corporations and interest groups—the right and ability to participate, enables them to form new groups better suited to address new problems. Alone, there is not much any person can do to bring about change or to participate meaningfully and usefully in a policy-making process. But working together as a group can take meaningful action. Online groups can also change their collective goals in response to pressing problems more quickly than traditional organizations that lock in their own institutional and individual priorities.

Government need not—it must not—fear new technology and the opportunity it creates, to invite participation from those with the experience in the field. Reinventing democracy as collaborative democracy will create work for government. Having a blog requires someone to respond to comments. Posting a wiki demands following the changes as they evolve. Creating a web form to invite input from the public, necessitates honing in on the right questions and listening to the resulting answers. Participation will require staffing and technology to manage. But a collaborative culture does not place the burden on government or the public alone to address complex social problems. Instead, by organizing collaboration, government keeps itself at the center of decision-making as the neutral arbiter in the public interest and also benefits from the contributions of those outside of government. Joseph Nye explains the collaborative imperative for governments:

> The very nature of leadership has changed in today's interdependent, globalized world. In information-based societies, networks are replacing hierarchies, and knowledge workers are less deferential. Business is changing in the direction of "shared leadership" and "distributed leadership," with leaders in the center of a circle rather than atop a hierarchy… Modern leaders need an ability to use networks, to collaborate, and to encourage participation. They need to be able to make decisions within rapidly changing contexts. They need to attract followers into new identities—both individual and social—and provide meaning in a disruptive world of globalization. In short, they need to use the soft

> power of attraction as well as the hard power of force and threat, both at home and in foreign policy.[54]

In other words, collaboration offers a huge potential payoff in the form of more effective government. Effective government, in turn, translates into better decision-making and more active problem solving, which could spur growth in society and the economy.

Let's say that the Environmental Protection Agency wants to pass a regulation protecting a certain endangered species. As currently designed, public input comes too late for anyone but a lobbyist to effectively have a say. But the Internet makes it possible to design methods for soliciting better expertise sooner from private citizens. Or imagine that the United States Postal Service wants to cut its energy bills by 30% over the next 3 years. An online best-practices website would enable the USPS to generate many solutions from crowds of people. Those crowds could include self-selected experts across federal, state, and local government as well as motivated members of the public. Imagine that a series of economic events triggers a crisis of confidence in the economy. Technology could make it possible to track economic data in a more transparent, collaborative, verifiable way.

Innovation in the practices of governance will require investment. But if government can design effective mechanisms—law, policy, and technology—to build the bridge between institutions and networks, it can enhance its legitimacy and value. Look what happened to the entertainment industry. Fearing a loss of ad revenue from consumers' home taping, the movie studios and television broadcasters initially feared the new tools. They (unsuccessfully) sued the makers of the Betamax personal video recorders (the precursor of the DVD and the VCR) in an effort to put the consumer electronics companies out of the Betamax business altogether.[55] People wanted to watch movies at home and would not be stopped. Eventually, the home video rental market, far from threatening the incumbents, flourished and vastly increased their markets.

Similarly, in response to the advent of digital technologies that reduce the cost of making and distributing nearly perfect copies of music, the record labels proposed legislation to criminalize new forms of copyright infringement. They began suing 12-year-olds and grandmothers for illegally sharing music files via peer-to-peer networks and filed suit to put the makers of these new digital technologies out of business.[56] But the law is out of step with society's music consumption practices: while traditional business models wane, iTunes, eMusic and other alternatives innovate and embrace the power of new technology. Instead of cheating or routing around the music laws, these new entrants are helping to reengineer and

---

[54] Nye 2008.

[55] Sony Corp. of America. Universal City Studios, 464 U.S. 417 (1984).

[56] Prioritizing Resources and Organization for Intellectual Property Act of 2008 (ProIP Act) S. 3325; Anderson 2008b, Borland 2003, Bangeman 2007. See also *MGM Studios Inc.* v. *Grokster, Ltd.*, 545 U.S. 913 (2005) (peer-to-peer file-sharing case), and also http://arstechnica.com/old/content/2005/06/5042.ars

reshape the industry. If institutions do not work with the networks, networks will work around them, rendering government practices increasingly disconnected, ineffectual, and brittle.

References

Ackerman BA, Fishkin J (2004) Deliberation day. Yale University Press, New Haven
Anderson H (2008a) Intellectual property and free expression. Lecture, Stanford University, 27 May 2008 (notes on file with author)
Anderson N (2008b) Big content gloats as Bush signs Pro-IP Act. Ars Technica, 14 October 2008. http://arstechnica.com/news.ars/post/20081014-bush-signs-pro-ip-act-big-content-gloats.html
Ashcroft J (2001) The Freedom of Information Act. Memorandum for all heads of departments and agencies. 12 October 2001
Baker M, Mozilla Foundation chairman of the board (2008) Summer 2008 Goals. 14 May 2008. http://blog.lizardwrangler.com/2008/05/14/
Balkin JM (2004) Digital speech and democratic culture: a theory of freedom of expression for the information society. N Y Univ Law Rev 79:1–58
Bangeman E (2007) RIAA versus grandma, Part II: the showdown that wasn't. 16 December 2007. http://arstechnica.com/tech-policy/news/2007/12/riaa-versus-grandma-part-ii-the-showdown-that-wasnt.ars
Barber BR (1984) Strong democracy. Princeton University Press, Princeton, NJ
Bohman J (1996) Public deliberation: pluralism, complexity, and democracy. MIT Press, Cambridge, MA
Borland J (2003) RIAA settles with 12-year-old girl. 9 September 2003. http://news.cnet.com/2100-1027-5073717.html
Chadwick A (2006) Internet politics: states, citizens, and new communications technologies. Oxford University Press, Oxford
Collins ED (1901) Committees of correspondence of the American revolution. Annual report of the American Historical Association, pp 245–271
Cowell FR (1975) The Athenaeum: club and social life in London. Heinemann, London
Cronin TH (2006) Direct democracy: the politics of initiative, referendum, and recall. Harvard University Press, Cambridge, MA
Czapanskiy K, Manjoo R (2008) The right of public participation in the law-making process and the role of the legislature in the promotion of this right. Univ Md School of Law Leg Stud 42:31
Fishkin JS (1991) Debating democracy and deliberation: new directions for democratic reform. Yale University Press, New Haven
Fountain H (2008) A cloth to cut the mercury risk from lightbulbs. New York Times, 8 July 2008
Gerth HH, Wright Mills C (eds) (1991) From Max Weber: essays in sociology. Routledge, London
Guimary D (1975) Citizens groups and broadcasting. Praeger, New York
Gup T (2007) Nation of secrets: the threat to democracy and the American way of life. Doubleday, New York
Kiel P (2007) Bush admin: what you don't know can't hurt us, 2007 Version. 23 November 2007. http://tpmmuckraker.talkingpointsmemo.com/archives/004766.php
Kosslyn SM (2006) On the evolution of human motivation: the role of social prosthetic systems. In: Platek SM et al (eds) Evolutionary cognitive neuroscience. MIT Press, Cambridge, MA
Krauthammer C (1992) Ross Perot and the call in Presidency. Time, 13 July 1992
Lunder S, Houlihan J (2008) EPA Axes Panel Chair at request of chemical industry lobbyists. March 2008. http://www.ewg.org/reports/decaconflict

Macintosh A, Coleman S (2003) Promise and problems of E-democracy: challenges of online citizen engagement. OECD
Meiklejohn A (1960) Political freedom: the constitutional powers of the people. Harper, New York
Meskell D (2007) New opportunities for involving citizens in the democratic process. USA Services Intergovernmental Newsletter 20:1–3. http://www.usaservices.gov/events_news/documents/USAServicesNewsletterFall-07.pdf
Miller E (2008) You can markup the bills on the mortgage industry bail out. 22 September 2008. http://blog.sunlightfoundation.com/2008/09/22/
Mooney C (2005) The Republican war on science. Basic Books, New York
More People See Federal Government as Secretive; Nearly All Want to Know Where Candidates Stand on Transparency (2008) Sunshine Week, 15 March 2008. http://www.sunshineweek.org/sunshineweek/secrecypoll08, Accessed October 2008
Mutz DC (2006) Hearing the other side: deliberative versus participatory democracy. Cambridge University Press, New York
Newport F (2008) Bush's 69% job disapproval rating highest in Gallup history. 22 April 2008. http://www.gallup.com/poll/106741/bushs-69-job-disapproval-rating-highest-gallup-history.aspx
Noveck BS (2005) A democracy of groups. First Monday, December 2005. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1289/1209
Noveck BS (2009) Wiki government: how technology can make government better, democracy stronger and citizens more powerful. Brookings Institution Press, Washington, DC
Nye J (2008) Picking a President. Democracy J Issue 10 Fall 2008:19–28
Oram A (2007) In search of microelites: how to get user-generated content. 14 November 2007. http://radar.oreilly.com/2007/11/in-search-of-microelites-how-t.html
Page SE (2007) The difference: how the power of diversity creates better groups, firms, schools and societies. Princeton University Press, Princeton, NJ
Ruhl JB, Salzman J (2006) In defense of regulatory peer review. Wash Univ Law Rev 84:1–61
Sapien J (2008) Industry-packed Federal Advisory Board told DOE to double U.S. coal consumption. 19 May 2008. http://www.propublica.org/article/industry-packed-federal-advisory-board-told-doe-to-double-us-coal-consumpti
Schudson M (1998) The good citizen: a history of American civil life. Free Press, New York
Sclove RE (1996) Democracy and technology. Guilford, New York
Shane PM (ed) (2004) Democracy online: the prospects for political renewal through the Internet. Routledge, New York
Skocpol T, Fiorina MP (eds) (1999) Civic engagement in American democracy. Brookings, Washington, DC
Sorkin M (2003) Starting from zero: reconstructing downtown New York. Routledge, New York
Sunstein C (2003) Why societies need dissent. Harvard University Press, Cambridge, MA
Terkel A (2008) Bush administration hides more data, shuts down Website tracking U.S. economic indicators. 13 February 2008. http://thinkprogress.org/2008/02/13/economic-indicators
Tetlock PE (2005) Expert political judgment: how good is it? How can we know? Princeton University Press, Princeton, NJ
Union of Concerned Scientists (2005) Restoring scientific integrity in policy making: scientists sign-on statement. 8 February 2005. http://www.ucsusa.org/scientific_integrity/abuses_of_science/scientists-sign-on-statement.html
Union of Concerned Scientists (2008) Interference at EPA: science and politics at the U.S. environmental protection agency. 23 April 2008. http://www.ucsusa.org/scientific_integrity/abuses_of_science/interference-at-the-epa.html
Volokh E (2001) How might cyberspace change American politics. Loyola Los Angel Law Rev 34:1213–1220
Wald M (2007) A U.S. alliance to update the lightbulb. New York Times, 14 March 2007

Wooley AW et al (2007) Using brain-based measures to compose teams: how individual capabilities and team collaboration strategies jointly shape performance. Soc Neurosci 2:96–105

Wyatt E, Bagli CV (2002) Visions of ground zero: the public; officials rethink building proposal for ground zero. New York Times, 21 July 2002

Zinn H (2007) A power governments cannot suppress. City Lights, San Francisco

Chapter 7
Electronic Voting: Approaches, Strategies, and Policy Issues—A Report from Switzerland

Urs Gasser and Jan Gerlach

Contents

7.1 Introduction 102
7.2 Overview 102
7.2.1 Approach 102
7.2.2 Pilot Projects 104
7.2.3 Basel-Stadt 107
7.2.4 Conclusions 107
7.3 Policy Issues: Theory and Practice 108
7.3.1 Participation 108
7.3.2 Autonomy 112
7.3.3 Quality 114
7.3.4 Conclusions 116
7.4 Institutional Framework for e-voting Systems 117
7.4.1 Design Challenge 117
7.4.2 Design Elements 118
7.5 Conclusion 126
References 127

Contribution received in 2010.

U. Gasser (✉)
Berkman Center for Internet and Society, Harvard University, Cambridge, MA, USA
e-mail: ugasser@cyber.law.harvard.edu

J. Gerlach
Research Center for Information Law, The University of St. Gallen, St. Gallen, Switzerland
e-mail: jan.gerlach@unisg.ch

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_7,

7.1 Introduction

The long-term effects of the Internet on political systems and underlying information processes remain uncertain and are the subject of a new strand of multidisciplinary—and increasingly quantitatively oriented—research. While the jury is still out, anecdotal and in some cases even empirical evidence from various countries suggest shifts in the ways in which political rights are exercised in the digitally networked environment. Much attention has been paid to the use of digital tools with regard to political campaigns—especially in the context of the recent US presidential campaigns, but also with the role of the Internet in South Korea or during the Ukraine's Orange Revolution. Admittedly less spectacular and less transformative is the use of the Internet in the context of the voting process itself, which in democratic societies is considered to be a core element within the suite of political rights. Several countries in the Western hemisphere, including Canada, Estonia, the United Kingdom, the United States, and Switzerland have acquired some initial experience with Internet voting as a subcategory of a broader set of distant-voting techniques. This article provides an overview of the Swiss experience with e-voting by looking at the respective projects in the cantons of Geneva, Zurich, Neuchatel, and Basel-Stadt, and surveys the key promises and challenges, both from a theoretical and practical perspective. Finally, the article discusses selected legal, technological, and social factors that need to be taken into account and managed when building an institutional framework for e-voting.

7.2 Overview

7.2.1 Approach

Looking from a bird's-eye perspective, one of the key features of the Swiss e-voting ecosystem is the way in which it has emerged[1]: it has been (and continues to be) built both in a bottom-up and decentralized manner—an approach that is not only consonant with Swiss culture and the prevailing legal (federalist) framework, but is also a practical necessity vis-à-vis a country with 26 cantons and different corresponding voting systems, which can also vary among municipalities within a single canton. However, 'decentralized' does not mean uncoordinated. An e-voting initiative was launched in the context of the Federal Council's 'Strategy for an Information

[1] In this article, we use the terms 'e-voting' and 'Internet voting' as synonyms for the act of casting a ballot through a secure channel over the Internet. Swiss authorities often use the French term 'vote électronique,' which is broader in the sense that it not only describes the actual casting of a ballot, but also the general exercise of political rights practiced in Switzerland, such as the signing of initiatives (i.e., proposal for a new article of the constitution or of a law) and referenda (i.e., challenge of a law passed by the parliament) as well as the dissemination of information about votes and elections on behalf of authorities. See Federal Council 2002, p. 651.

Society' of 1998 and 2006, respectively,[2] and started in 2001 and 2002 with a series of pilot projects in the cantons of Geneva, Zurich, and Neuchatel. The three cantons volunteered and signed contracts with the Federal Chancellery to conduct legally binding tests of e-voting systems during federal polling. The goal was to gain experience and know-how in Internet voting and set the stage for a larger political debate about the introduction of e-voting in Switzerland (Braun 2004). The agreement stipulated a series of principles and security requirements, clarified that the cantonal experiments did not prejudice a federal solution further down the road, and included a commitment by the federal government to cover up to 80% of the extra costs associated with the e-voting experiments. It was also agreed that the results of the pilot projects would be made available to all other cantons.[3] The necessary adjustments of the legal framework at the federal level—including a revision of the Federal Act on Political Rights of 17 December 1976[4]—followed suit. In January 2003, the first votes were cast through remote electronic means in a municipal ballot in Anières, a town in the canton of Geneva. Another milestone was met in 2004, when e-voting became available for the first time for federal and cantonal ballots in selected municipalities of the canton of Geneva. Municipalities in Zurich and Neuchatel followed in 2005. The series of pilot projects coordinated at the federal level concluded in 2006. In its report that marked the conclusion of the pilot projects, the Federal Government deemed the tests a success and opined that there was neither reason to stop further tests nor to hastily extend them.[5]

The pilot projects in the three cantons focused on citizens living in Switzerland. However, the use of the Internet as a means to exercise one's political rights seems even more promising for citizens who live outside their home country. Given the large number of Swiss citizens abroad—more than 10% of the Swiss population[6]—and the manifold challenges associated with exercising political rights from afar, it is not surprising that the Federal Council considered Swiss people living abroad a core constituency for e-voting[7] and decided to move forward in making e-voting available to them.[8] By implementing this strategy, the legal provisions governing voting by Swiss citizens living abroad—the Act on Political Rights of Swiss Living Abroad—were amended in 2007. One year later, Neuchatel was the first canton to allow its registered citizens living abroad to vote online. In November 2009, the canton of Geneva's e-voting infrastructure was used by the canton of Basel-Stadt, which provided e-voting exclusively to its registered citizens living abroad. This first

[2] Strategy of the Federal Council for an Information Society in Switzerland 1998; Strategy of the Federal Council for an Information Society in Switzerland 2006.

[3] See http://www.bk.admin.ch/themen/pore/evoting/00774/index.html?lang=de

[4] Unofficial English translation available at http://www.bk.admin.ch/themen/pore/index.html?lang=en&download=M3wBPgDB_8ull6Du36WenojQ1NTTjaXZnqWfVp3Uhmfhnapmmc7Zi6rZnqCkkIR6e3p_bKbXrZ6lhuDZz8mMps2gpKfo

[5] Federal Council 2006a.

[6] See http://www.aso.ch/de/information/statistik

[7] Federal Council 2006a, p. 5533.

[8] Federal Council 2006b, p. 5303.

occasion in which one canton hosted another canton's ballot was considered a success.[9] In 2010 and 2011, more cantons will follow the example of Basel-Stadt and allow Swiss citizens living abroad to vote online via Geneva's e-voting platform.[10]

Moving forward, the Federal Chancellery has outlined an ambitious agenda: According to one document, the Federal Chancellery aims to provide an e-voting infrastructure to a subset of Swiss citizens living abroad for the elections of the Federal Parliament in 2011. According to this plan, 50% of this population should be able to cast their vote online in 2012, while a majority of them will be able to take part in the national elections of 2015.

7.2.2 Pilot Projects

7.2.2.1 Geneva

The Canton of Geneva is the pioneer canton when it comes to Internet voting. It started to develop its e-voting system in 2000[11] and has probably the broadest worldwide experience in the field when looking at the numbers of binding decisions taken by the electorates (Alvarez et al. 2009). A couple of reasons made Geneva a 'designated candidate' for the introduction of e-voting (Geser 2002). First, the canton of Geneva has a centralized electronic voting registry. Swiss law requires citizens to register with local authorities, but often, registries have not been interconnected and computerized. In the canton of Geneva, by contrast, which happens to have only a small number of municipalities, local voters' registries had been electronically linked even before the start of the e-voting project.[12] This has made the authentication process—one of the key challenges in any e-voting setting—much easier. Second, the voting law that dates back to 1982 authorized the cantonal authorities 'to collaborate with the municipalities in trying out new voting methods at variance with the present law, in order to bring voting procedures in line with new technological conditions.'[13] This created the

[9] See http://www.geneve.ch/evoting/communiques_20091129.asp

[10] See http://www.geneve.ch/evoting/english/presentation_projet.asp

[11] Ibid.

[12] Swiss law requires citizens to register with local authorities. Most often these registries have not been interconnected.

[13] Art. 188 Loi sur l'exercice des droits politiques du 15 octobre 1982 [Law on Political Rights from 15 October 1982]: 'Departure from the law: For cantonal or municipal issues, the government may, in accordance with the concerned municipalities, depart exceptionally and in a limited way from the rules enshrined in the law on political rights and describing the ways these rights must be exercised and the ballots be counted, in order to allow for testing new ways of political expression that technical developments make possible.' [as translated by the State Chancellery of Geneva in the official invitation of tender for the development of the e-voting platform].

possibility for experimentation without requiring a time-consuming legal reform process. Third, the citizens of the canton of Geneva have a long and strong track record in distant voting. Within eight years after the introduction of the absentee vote by mail, more than 90% of Geneva's citizens had turned to postal submission of their votes. Thus, most of the voters were already used to voting from the privacy of their homes as opposed to going to the ballot boxes (or even publicly casting their votes at an assembly as in more traditional Swiss cantons).

The first time e-voting was made available by the cantonal government was in January 2003, when a little over 1,000 citizens of Anières were able to cast a municipal ballot online. After testing the system in three more municipal ballots, the canton of Geneva enabled e-voting for cantonal and federal ballots for the first time in September 2004 in the municipalities of Anières, Carouge, Cologny, and Meyrin.[14] The second federal ballot using the new voting method took place in November 2004 when a total of 41,200 citizens[15] from Anières, Carouge, Cologny, Collonge-Bellerive, Meyrin, Onex, Vandoeuvres, and Versoix were given the possibility to vote online. Subsequently, e-voting was enabled for ballots in April 2005 and in November 2008 with fourteen and nine municipalities respectively taking part.[16] In September 2009, votes were cast for the 12th time over the Internet (including municipal ballots), while another premiere took place: for the first time, e-voting became available to citizens living abroad.[17]

7.2.2.2 Zurich

Unlike Geneva, the Canton of Zurich does not have a centralized voter registry. Rather, voters are registered within their local municipalities, which maintain their registries independently, use separate information systems, and perform separate vote tallies. Given this lack of interoperability, the Zurich e-voting model has perhaps been the most challenging one from an organizational and technical angle. It had to deal with the fact that there was no centralized database for voter authorization. Initially, the creation of a canton-wide, shared database that would be constantly updated by the municipalities came under consideration (Braun 2004). The current system, however, follows a different approach by retrieving voter registration data from the respective computer systems of the various towns and communities within the canton. Thus, rather than building a long-term central

[14] See http://www.geneve.ch/evoting/english/historique.asp

[15] Ibid.

[16] In 2007, the government introduced a proposal to amend the law on political rights aimed at adding Internet voting as a regular voting channel. In order to make way for the parliamentary debate, e-voting was suspended between the introduction of the proposal and it's adoption (now in form of a constitutional amendment) in mid-2008, see http://www.geneve.ch/evoting/english/historique.asp

[17] See http://www.ge.ch/chancellerie/communiques/2009/20090903.asp

database for the entire canton, Zurich decided to download the current lists of registered voters at the time of an election or referendum (Braun 2004; Engi and Hungerbühler 2006).

Zurich launched the e-voting project in May 2001 and started its implementation in the fall of 2003. After a number of tests, including a student parliament vote at the University of Zurich, the e-voting trials started with a municipal vote in the town of Bülach in October 2005. Just one month later, citizens in the towns of Bertschikon, Bülach, and Schlieren had the possibility to cast their votes online in a federal and cantonal ballot. The test series was officially concluded in 2006. Since then, the e-voting system has been available to citizens of the three aforementioned municipalities, and the system was extended to nine additional municipalities for a September 2008 ballot. Shortly thereafter, parts of the city of Zurich were also included. In 2010, the government committed to provide e-voting to Swiss citizens living abroad who are registered in the canton of Zurich. Before 2012, however, the system is not expected to be extended again (Bosshard et al. 2008).

7.2.2.3 Neuchatel

The e-voting pilot project in the canton of Neuchatel has been part of a broader cantonal initiative called 'Guichet Unique.' The basic idea of this 'virtual government window' is to create a one-stop-portal for information and services offered by the regional and local government. It can be used for a broad range of transactions, including tax management, birth registration, change of address notification, requests of certificates, or license plates for cars.[18] The portal consists of various elements, including an authentication system.

In September 2005, the first votes were cast electronically in a federal ballot. One month later, the 'Guichet Unique' was used in a cantonal ballot. The most recent vote of November 2009 represented the 12th time, that e-voting was used in official ballots in the canton of Neuchatel. Unlike the e-voting project of Geneva, which so far restricts e-voting to certain municipalities; Neuchatel's project limits the number of e-voters to a certain overall number that is determined by the Federal Council. The original limit (set by the Federal Council) on the number of citizens that are allowed to vote electronically has been increased over the years from 4,000 in 2006 to 12,000 in 2009.[19] The most recent increase reflects the fact that Swiss citizens living abroad and registered in Neuchatel were also permitted to cast their vote online.[20]

[18] See http://www.bk.admin.ch/themen/pore/evoting/00774/00781/index.html?lang=de

[19] Federal Council 2009a.

[20] Federal Council 2009b.

7.2.3 Basel-Stadt

As mentioned above, Basel-Stadt is the first canton that introduced e-voting and has not been a part of the pilot series outlined in the previous section. In November 2009, Basel-Stadt provided Swiss citizens living abroad who are registered in the canton the possibility to cast their votes online. The poll, which was conducted without any technical problems, was considered a success by both the canton[21] and the voters.[22]

This most recent e-voting project is interesting in at least two aspects. First, the key elements of the voting infrastructure were provided and hosted by the canton of Geneva, which adds an additional level of legal and institutional complexity as further discussed below. In any event, this outsourcing-approach, which is currently being considered by other cantons as well, very much corresponds with the Federal Council's original plan; in light of the costs of e-voting projects, the Council proposed very early on that not all cantons develop their own e-voting system, but rather make use of the ones tested in the three pilot projects.[23]

The second distinct feature concerns the fact that Basel-Stadt only permitted Swiss citizens living abroad to cast their vote online, in contrast to the trials discussed before. In March 2010, Swiss citizens abroad will again be able to cast their vote online. Whether e-voting will be extended to the resident citizens will be decided by the cantonal Government in approximately two years time.[24]

7.2.4 Conclusions

Switzerland has taken an interesting and measured—one might even say: cautious—conceptual approach to the introduction of e-voting. While part of a national strategy and with its foundation in the federal legislative framework, three volunteering cantons have developed the core e-voting infrastructure in a decentralized and distributed way, albeit in close coordination with the federal authorities. A brief overview suggests that such an approach is not only consonant with Switzerland's federal structure, legal set-up and cultural characteristics, but actually has also led to favorable results: The three pilot cantons have successfully implemented e-voting systems by pursuing quite different strategies—some of them more holistic, others more specific—and by using different technological designs as further discussed below. As a result, a rich set of technical, legal, organizational, and human experience has become available—a much richer set

---

[21] See http://www.regierungsrat.bs.ch/staatskanzlei/e-voting

[22] See a survey conducted among the people who cast their vote online, available at http://www.regierungsrat.bs.ch/e-voting-umfrage-09-11-29.pdf

[23] Federal Council 2006a, p. 5527.

[24] See http://www.regierungsrat.bs.ch/staatskanzlei/e-voting.htm

than the outcome of a possible alternative, top-down or single-pilot strategy. The recent move by the canton of Basel-Stadt to introduce e-voting by using the infrastructure of the canton of Geneva—an interesting case of 'infrastructure shopping' among cantons—is early evidence of the promises of such a coordinated, but highly decentralized bottom-up approach in a federal democratic system like Switzerland.

7.3 Policy Issues: Theory and Practice

Internet voting comes, both with manifold opportunities and probably even a larger number of challenges at various levels. In its preliminary report[25] on e-voting, the Federal Council named better facilitation of suffrage, faster supply of voting information, an augmentation of the participation rate, and better interpretation of ballots by electronic means to be some of the potential benefits of the introduction of the 'vote électronique.' But the federal government has also pointed out the risks, which include a potential participation gap as a result of the digital divide, the de-ritualization of political rights, shorter processes of opinion formation, information overload, and security risks.

In this section, we focus on three important policy clusters—participation, autonomy, and quality—and discuss and contrast some of the most frequently mentioned promises as well as challenges of e-voting against the backdrop of the Swiss experience. In most instances, we do not have sufficient data to make general claims or draw reliable conclusions, but the discussion might at least shed light on some of the key considerations that need to be taken into account when evaluating the promise and limits of Internet voting from a public policy perspective.

7.3.1 Participation

7.3.1.1 Opportunities

Switzerland has one of the lowest levels of voter turnouts among established democracies, while Swiss voters are among those citizens who are most frequently (at least four times a year) called to the polls (Trechsel 2007). Several theories and models have emerged, that aim to explain why some citizens participate in political processes through voting and others do not. Among the factors frequently mentioned across various models is the cost of participation: the higher the costs associated with access to the ballots, the lower the likelihood of participation,

[25] Federal Council 2002, p. 645.

according to this hypothesis. Against this backdrop, various forms of remote (or absentee) voting aimed at lowering transaction costs have been explored and adopted, with e-voting as the most recent and perhaps most promising candidate. In addition to transaction cost arguments, the promise of e-voting systems has been linked to particular audiences such as young voters with strong Internet-affinity, elderly people because of their limited mobility, Swiss citizens living abroad given mail delivery issues, and blind or visually impaired people (Braun and Brändli 2006).

Against this theoretical backdrop and in light of earlier experiences with postal voting in Switzerland, which resulted in an increase of turnout rates (according to some analyses by up to 20 percentage points),[26] it was expected that the introduction of e-voting would also result in an increased participation level. This expectation was reinforced by a number of surveys both at the national[27] and cantonal level (Trechsel 2007), indicating that the "convenience factor" of e-voting makes it particularly attractive for citizens. Somewhat in contrast to these findings, the Federal Council has remained sceptical about the potential of e-voting as a means to increase voter turnout.[28]

As of today, it remains difficult to determine whether e-voting in Switzerland increases participation or not. One of the most interesting studies was conducted in the context of the Geneva pilot project. Researchers calculated the difference between the cantonal average in turnout for eleven votes held between 2001 and 2004 and the mean turnout for the votes in the four communities in which e-voting was subsequently offered. The study found only small differences in turnout—but contrary to the expectation, the four communities showed lower turnout rates once e-voting was introduced. The authors of the study convincingly argued that little can be concluded based on these findings. Since e-voting is introduced as a complementary and not a substitutive form of voting, it should not have a negative effect on voter turnout. While the 'results prevent any form of immediate enthusiasm concerning some turnout-boosting effect of e-voting … one needs to adopt a longer term perspective in order to solidify such a statement based on aggregated data' (Trechsel 2007).

Additional insights can be gained from a survey conducted in the context of a 2004 e-voting trial in four Geneva communities (Trechsel 2007). According to the study, citizens who can be described as occasional voters were the most likely to be attracted to and mobilized through the introduction of e-voting. This suggests that any substitution effect that e-voting might have may affect other remote voting methods as opposed to traditional forms of ballot casting. The survey not only focused on turnout, but also assessed qualitative shifts when moving from traditional modes of participation to e-voting. Surprisingly, a combined socio-economic,

[26] See http://www.geneve.ch/evoting/english/presentation_projet.asp. However, the effects of postal voting on voter turnout are not as clear as this number might suggest, see Franklin 2004, p. 156 et seq. [cited in Trechsel 2007, p. 162.].

[27] Gfs.bern 2005, p. 34.

[28] Federal Council 2006a, p. 5503.

demographic and ICT model analysis suggests that neither age nor income were statistically significant factors in the September 2004 Geneva e-voting pilots. Similarly, e-voting has reportedly not increased participation among young voters in the canton of Neuchatel; the 30 to 65-year-olds were among the most frequent users of Internet voting (Rota 2008). The only significant variable in the Geneva context was associated with ICT-related factors. The findings suggested the following relationship: 'the higher the computer literacy, the faster the internet connection; the higher the level of trust in communications over the internet and the higher the trust in e-voting procedure itself, the higher the probability of a voter to prefer e-voting over traditional channels of participation' (Trechsel 2007).

Given the limited data that is currently publicly available, it is important to note that the quantitative and qualitative effects of e-voting on participation are both context and design-specific. Several surveys suggest, for instance, that 'convenience' is one of the key drivers of e-voting take-up. Consequently, much depends on the particular design of the e-voting system, especially vis-à-vis the relatively high user-friendliness of postal voting. Contextual factors matter, too. For example, remote voting is particularly popular in the cities, while in rural, small villages, it is more common to walk to the ballot box.[29]

7.3.1.2 Challenges

E-voting not only shows promise, but also comes with challenges with regard to voter participation. The concern originates from a new type of gap that splits today's society into two parts: the digital 'haves' and digital 'have-nots.' Two related, but analytically distinct challenges can be identified with respect to this type of societal divide, which no longer only separates North and South, but has its demarcation line within a given region or country. The first issue has to do with citizens' access to broadband technology. The second dimension of the participation gap relates to knowledge and ability—or the lack thereof—which is required to understand and use digital technologies, including e-voting systems.

With regard to access to broadband technology, Switzerland has been in a relatively comfortable situation as recent studies demonstrate. Broadband penetration rates are high in Switzerland and prices for reasonable speeds are affordable when compared to other countries (Berkman Center 2009). Viewed from that perspective, access is currently not much of a concern in Switzerland. However, it should be noted that access may vary significantly among regions and is more limited in rural areas and in the mountain regions. Also, new inequalities may emerge in the future when moving to the next generation network with network upgrades and fiber-to-the-home deployment focusing on major cities. Nonetheless, given the current connectivity level and the statutory limitation on the percentage

[29] See a statistics bulletin on voters' habits in the canton of Zurich during the years 1994–1999, available at http://www.statistik.zh.ch/themenportal/themen/down.php?id=241&fn=1999_11.pdf.

of e-voters (federal law stipulates an e-voting cap of 10% of all eligible voters throughout the nation),[30] it seems rather unlikely that a significant number of citizens are at a disadvantage under an e-voting regime. Looking at participation more broadly, we also need to keep in mind that e-voting will not replace traditional forms of voting in the foreseeable future, but is considered to be an additional voting channel. On the other hand, one might expect that even relatively marginal access limitations (e.g., access from public places *versus* access from home) may have a negative impact on the popularity of e-voting systems and hamper its potential to increase voter turnout.

Less data is available on the second aspect of the participation gap: digital literacy. The fact that two-thirds of Switzerland's population already use the Internet suggests that basic computer and Internet skills are widespread[31]—although the skills that are required to understand and successfully navigate an e-voting system are likely to vary substantially across the different systems that have been developed, as a quick look at the respective user-interfaces reveals. Even if we assume that the two-thirds who use the Internet are automatically also savvy users of e-voting systems, it obviously leaves one-third of the population without Internet experience. We do not know enough about the overlap between the demographics of people offline and the demographics of potential e-voters to draw conclusions on how this participation gap may play out in terms of voter turnout in an e-voting environment, but it seems safe to hypothesize that lack of skills might be another relevant factor that limits the potential positive effect of e-voting.

One interesting approach that may have addressed at least some of these concerns was developed—but later abandoned—by the canton of Zurich. The Zurich model's early experiments with voting through SMS (text messaging) not only expanded the convenience of e-voting, but may also have had the potential of closing the participation gap, since more eligible voters seem to own a cell phone than have ready access to the Internet.[32]

---

[30] Art. 27c subpara 2 Ordinance on Political Rights.

[31] See http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html?open=1#1

[32] Just over 2 million broadband connections were reported in Switzerland for the year 2006. 'Breitbandmarkt,' http://www.comcom.admin.ch/dokumentation/00439/00565/index.html?lang=de. In contrast, there were reportedly over 7 million cell phone numbers in use in Switzerland in that same year. 'Mobilfunkmarkt,' http://www.comcom.admin.ch/dokumentation/00439/00467/index.html?lang=de. Additionally, a survey following the November 2007 e-voting trials in Bertschikon revealed that 79% of respondents owned and used a mobile phone, whereas only 38% had internet access at home with an additional 8% who only had access at work. Eicholzer 2006. The SMS voting services were discontinued in 2007 after they proved to be particularly unpopular: Government Council, Canton of Zurich 2007. A more significant percentage of voters in Bertschikon utilized the SMS option, yet usage of the SMS option dropped significantly in Bülach between the original October trial and the November referendum. See Prader 2006, slides 24–25 (on file with authors). And for local elections in April 2006, only 0.8% of voters in Bülach chose the SMS option. 'Behördenwahlen Bülach vom 2. April 2006' [Public elections in Bülach of 2 April 2006], http://www.statistik.zh.ch/produkte/evoting/buelach020406.pdf.

7.3.2 Autonomy

7.3.2.1 Opportunities

Switzerland's legal framework concerning political rights is designed, inter alia, to ensure its citizens' autonomy when it comes to the exercise of political rights through the act of voting. Among the guiding principles aimed at securing the voter's autonomy are the requirements of secret and free suffrage as stipulated in the Federal Act on Political Rights. These principles also apply to e-voting, and through very detailed amendments to the Ordinance on Political Rights, the Swiss legislature has translated them from the analog to the digital voting environment. An overview of the detailed provisions suggests that the federal lawmaker, by and large, has regarded e-voting to be a phenomenon that puts autonomy at risk. Almost a dozen detailed provisions seek to guarantee the secret suffrage, and half a dozen requirements are aimed at safeguarding free suffrage (Braun 2004).

Given this perception and focus on threat scenarios, it is not surprising that little attention has been paid to the question whether e-voting systems—if designed creatively and implemented properly—could in fact enhance user autonomy. Looking at the secrecy requirements in the Ordinance on Political Rights (take encryption as an example), one might start questioning the existence of offline equivalents and the reliability of the corresponding measures for, say, postal voting. A second example: the Ordinance requires that the e-voting system explicitly draws a voter's attention—prior to voting—to the fact that she is officialy participating in a ballot. Arguably, such a reminder aimed at creating a moment of autonomous self-reflection does not necessarily find an offline equivalent. Several more examples of this sort could be added in order to illustrate that e-voting systems may indeed come with opportunities for enhancing citizens' autonomy given the rich set of design choices available.

While these opportunities largely depend on the particular software and platform design, and intersect with the issue of voting quality as further discussed below, e-voting systems may yield a more direct autonomy-enhancing effect with regard to certain groups and communities within a given society. The Federal Act on Political Rights, for instance, obliges the cantons to assist citizens with disabilities in the exercise of their political rights. For this constituency, the possibility of casting a ballot online can prove to be a major improvement of their capacity to exercise their political rights and therefore enhance their autonomy in no small way. Along similar lines and as illustrated by the Swiss experience, e-voting may help citizens living abroad to exercise their political rights. Especially citizens living in regions with poor postal services might benefit from the possibility of voting online as they depend less on timely and reliable delivery of postal mail.

This positive effect of casting the vote online is impaired by the fact that—at least as of now—voting materials (information and security codes) are still distributed by postal mail. Thus, envelopes containing voting information can still be

subject to delays or, worse, might be lost in delivery or stolen out of mailboxes; the confidentiality of the ballot as guaranteed by federal law may be at risk in such circumstances.[33] However, with regard to this particular risk, e-voting does not differ from the remote vote by postal ballot.

7.3.2.2 Challenges

As mentioned in the previous section, security, and confidentiality are among the top concerns when it comes to e-voting, as any violation of these principles violates fundamental rights and other legally guaranteed values, including citizens' autonomy.[34] The Swiss experience is illustrative of the broad range of scenarios and counter-measures that need to be taken into account to ensure that e-voting is secure and confidential. They range from a series of sophisticated legal safeguards such as the ones set forth in the Ordinance on Political Rights to organizational and technical measures.

Various threat scenarios can be distinguished.[35] For instance, e-voting systems must be secured against acts of manipulation. The lack of a hand-written signature (which is required for offline voting) increases the risk that the e-voter is not actually the person that she represents herself to be. While there has been some scepticism about the maturity of e-voting technology to ensure security at the beginning of the project,[36] there have been no reports of attempts at voting manipulation.[37] Still, various security issues continue to exist (Oppliger 2008), including spoofing, danger of abuse, misuse or breakdown of the system. As the Federal Council admits, e-voting—not unlike postal voting or voting at the ballot box—will never be completely safe from manipulation or unlawful observation.[38]

---

[33] Art. 5 subpara 7, Federal Law on Political Rights. See also Imhof 2006, who doubts that small municipalities will be able to provide their citizens living abroad with the secure infrastructure needed for e-voting.

[34] Concerns about the security of e-voting systems have been discussed by different groups such as the Chaos Computer Club (Chapter of Zurich), who has not taken any actions on this issue. See discussion of security concerns at https://zh.chaostreff.ch/E-voting.WA-CH, an association that opposes the introduction of e-voting, has contacted politicians and officials of e-voting projects criticizing the high costs of introduction. See the FAQs on their website at http://www.wach.ch/portrait/faq.htm

[35] For an overview on security issues and measures taken, see Braun and Brändli 2006, p. 33 et seq.

[36] Federal Council 2002, p. 658.

[37] See Federal Chancellery (a).

[38] Federal Council 2006a; see Postulat 09.3174—'Betrügerische Praktiken bei Wahlen und Abstimmungen?' [Fraudulent practices at elections and ballots?], http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20093174, and Interpellation 09.3573—'Rechtmässigkeit und Vertrauenswürdigkeit der brieflichen Stimmabgabe und des E-Votings' [Lawfulness and trustworthiness of postal voting and e-voting], http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20093573

Along the same lines, representatives of the canton of Geneva have pointed out that 'a secure e-Voting system must achieve an optimal trade-off between security of the procedure and user comfort' (Chevallier et al. 2006, p. 85). As a safeguard to ensure the quality of Swiss polls and elections in general, participation in e-voting on a federal level is currently restricted to 10% of all eligible voters throughout the nation.[39]

Another important, although more general threat category are viruses, trojan horses, and other types of malware. This type of badware not only compromises user autonomy and/or the quality of the decision-making process, but may seriously erode the trust in Internet transactions and communications in the first place. Given the important role that trust plays for the long-term success of e-voting systems, this set of challenges deserves particular attention; public policy-makers, Internet companies, NGOs, and individual users need to act in concert to address this problem, in the e-voting context and beyond.[40]

7.3.3 Quality

7.3.3.1 Opportunities

Internet voting can affect the quality of a vote in at least two analytically distinct ways. First, e-voting systems—if implemented properly—may increase the quality of the voting process at the aggregated level. As indicated in the previous paragraphs, legislators at both the federal and cantonal level as well as systems' designers and local authorities have come a long way to ensure that e-voting is as secure and reliable as the traditional voting methods. The design requirements for e-voting systems include, among other things, that only entitled voters may take part in a ballot; that no third party can systematically intercept, alter or divert electronic votes; that no third party can learn about the content of the votes cast; that the threat of systematic fraud is rendered impossible (Braun 2004; Burkert 2009). Looking at these and other requirements as well as at the sophisticated mechanisms of authentication and encryption, and taking into account the advantages of fully integrated, computer-based information processing (e.g., with respect to counting votes), one might speculate that the average quality of an Internet-based voting system in the Swiss context is likely to be as reliable and accurate in the long run as traditional systems, in which the human factor still plays a prominent role.

Second, the quality of the voting process can benefit from an electronic system at the individual level. E-voting systems in Switzerland have been designed in a way that voters have to confirm that their choice reflects their political

[39] Art. 27c subpara 2 Ordinance on Political Rights.

[40] See, e.g., http://www.stopbadware.org for an example of such a coordinated initiative.

determination before electronically submitting their vote. The interfaces and workflows, in accordance with legal requirements, have also been structured in such ways that voters are discouraged from voting precipitately or without reflection. Again, the three alternative designs in the pilot cantons illustrate that the current mechanisms might just be the starting place for more advanced mechanisms of quality control and quality-enhancing voting designs in the future. As early as 2002, for instance, the Federal Council suggested that through electronic evaluation of votes and comments, the population could gain more influence on decision-making, which would be a remarkable benefit for democracy.[41]

7.3.3.2 Challenges

As is the case in many other segments of the digital knowledge economy, there are also doubts about the potential of e-voting for raising the quality of votes and the quality of the voting process itself. While e-voting arguably has the potential to increase the quality of the votes submitted, it is not so clear whether the same is true for the quality of the information-based decision-making process leading up to the vote. Many of the concerns expressed in the literature are currently not backed-up by any of the (limited) data that is available, and in several instances the quality challenges assume a future in which e-voting is the exclusive means to exercise political rights. Regardless of the merits of these assumptions and claims, it is important to take note of these concerns in order to further analyze them over time and work towards solutions, where appropriate.

One cluster of quality concerns has to do with the ways in which official materials that seek to provide citizens with high-quality information and enable them to make informed choices, have been linked to traditional voting in Switzerland. In the case of a referendum, the executive branch of the government as well as the parliament distributes such information—including official recommendations—via mail together with the voting card. In an 'e-voting-only'-scenario, one could imagine that the government would disseminate the same materials by electronic means, for instance posting it on the e-voting website, which may increase the likelihood that voters would read this information given its context and timing. Critics, however, argue that this information would have less weight given all the other voices in cyberspace, including political parties and stakeholders of all sides of the political spectrum who represent manifold opinions and beliefs and make use of the new possibilities to advertise and propagate their message online at low costs, with negative consequences for the quality of the vote and ballot.

A related set of concerns adds a time-dimension to the quality challenge. According to this line of argument, the availability of diverse and competing political information online in tandem with an easily accessible e-voting infrastructure may reduce the depth of political discussion and interaction among

[41] Federal Council 2002, p. 654.

e-voters leading up to a poll. In this context, the Federal Council's report speaks of a 'de-ritualization' of the voting procedure.[42] In other words: while acceleration of the voting process certainly seems appealing to many people, it might also have a negative impact on the process of opinion formation. Observers coined the term 'fast-democracy' to describe this phenomenon.[43] According to this theory, people would not discuss their point of view with others over a longer period in a fully electronic environment.[44] Much to the contrary, e-voting only takes a minute or so, encouraging voting without much reflection or voting in an emotional (and irrational) state.[45] As a result, the quality of the vote might decrease, as voters might be more vulnerable to populism.

Another concern is the relative lack of transparency when it comes to the use of digital technology in voting procedures. In fact, 'processes of data generation, transformation, and storage occur in black boxes that are often not fully transparent even for the technical experts.'[46] This, in turn, can hamper the legitimacy of a ballot, especially (but not only) in cases where doubts emerge as to whether the system has worked flawlessly or not. However, it should be noted that federal and cantonal law and practice requires in-depth checks of the e-voting systems, before, during and after the vote. Whether such an expert-based approach aimed at fixing the transparency challenge may suffice, remains an open question—also from a legal perspective, as an interesting recent judgement from the German Bundesverfassungsgericht in the context of electronic voting machines illustrates.[47]

7.3.4 Conclusions

A brief overview of the opportunities and challenges associated with e-voting leaves an ambiguous impression. With regard to key public policy areas such as participation, autonomy and quality, the review suggests that e-voting systems and processes might make important positive contributions to society by strengthening democratic processes, but that they are also associated with serious challenges that deserve attention. Some of these challenges—including the problem of manipulation and fraud—are not qualitatively new; rather, they become more visible in a period of technological and institutional change.

The overview also reveals that even in Switzerland, a country with a relatively long experience with e-voting systems, only limited data is available that could

---

[42] Federal Council 2002, p. 655.

[43] Engi and Hungerbühler 2006, p. 21.

[44] Yannis Papadopoulos from University of Lausanne describes this to be a part of general privatization of political votes. Federal Council 2006a, p. 5495.

[45] Linder 2003, pp. 103, 114.

[46] Geser 2002 (online publication).

[47] See Burkert 2009, p. 114 et seq. with an analysis of possible ramifications for e-voting systems in the Swiss context.

serve as a solid basis for the evaluation of the pros and cons of e-voting. This holds particularly true for highly sensitive areas such as the security and confidentiality of e-voting. Earlier research regarding participation and voter turnout illustrates the enormous value of data, which not only enables a facts-based discussion about promises and challenges (something much needed, for instance, in the context of the quality debate), but also helps us to improve e-voting strategies, and systems and manage unavoidable risks appropriately and effectively, both in the offline and online environment.

7.4 Institutional Framework for e-voting Systems

7.4.1 Design Challenge

The discussion of selected policy issues in the previous section—several more could be added—already gives a sense of the manifold challenges that any e-voting system has to address at the technical, organizational, and legal level in order to guarantee what are considered to be the key principles of democratic elections and referenda in the Swiss (and European)[48] context. The following principles, inter alia, have been set forth in the Ordinance on Political Rights[49]:

- Only authorized voters can take part in the ballot;
- Each voter has one vote and can vote only once;
- Systematic interception, alteration, manipulation or otherwise decisively influencing the outcome of the ballot is prohibited;
- The content of the vote cast must remain a secret;
- All the votes cast are counted;
- Any systematic fraud is impossible.

The main tools available in order to safeguard these principles include legal and technological approaches to set the rules of the game. The discussion in the previous section also suggests that the strategies aimed at dealing with these challenges, to be successful, need to take into account democratic traditions, political culture, and corresponding social norms that shape the institutions, concepts, perceptions, and practices of voting within a society. Social norms are particularly interesting since they might have a significant impact on how new voting techniques are adopted and used in a given context. Conversely, the technological, legal, and educational setting may also influence such norms over time, as the history of Swiss voting techniques—including postal voting—in the next paragraph suggests. Against the backdrop of these and other forces (such as economic conditions or computer literacy) at play, in combination with the high symbolic

[48] See, e.g., Code of Good Practices in Electoral Manners (Opinion No. 190/2002) by the European Commission for Democracy through Law.

[49] Art. 27d Ordinance on Political Rights.

value of voting in any democracy, the introduction of e-voting systems becomes a multi-dimensional design challenge. The following section illustrates three of the key design factors that must be taken into account—and their interplay managed—when introducing and operating an e-voting system.

7.4.2 Design Elements

7.4.2.1 Legal Factors

Voting as a democratic institution is embedded in and interacts with a sophisticated set of legal provisions that can roughly be divided into the general legal framework on the one hand, and specific provisions aimed at setting the rules and standards for voting on the other hand. The introduction and operation of e-voting systems will very likely require the amendment of existing provisions or the enactment of new provisions in the second category. However, one should not underestimate the effects of the general legal framework, which sets the overall parameters and conditions for any e-voting system and may actually have a significant impact on the design of the system itself. An example along these lines is the existence and design of digital signature laws in combination with ID card frameworks.[50]

The case of Switzerland is illustrative for the changes of specific voting norms in order to enable and regulate (test) e-voting. The amendments of federal laws—the Federal Act on Political Rights and the Act on Political Rights of Swiss Living Abroad—have already been mentioned above. Further, quite detailed provisions have been incorporated into the Ordinance on Political Rights. First, the Ordinance stipulates the basic conditions of and procedures for e-voting pilot projects and subjects these to the approval of the Federal Council.[51] Second, it sets forth the principled requirements (mentioned above) that need to be fulfilled in order to obtain permission from the Federal Council for the e-voting system.[52] Third, the Ordinance provides a detailed list of measures designed to implement the principled requirements.[53] Fourth, it stipulates higher-level requirements regarding the state of technology.[54] Fifth, it defines procedures in case of problems with

[50] Estonia with its very advanced e-voting strategy is a great illustration here: Estonia not only passed a digital signature act, but also mandated and introduced a national identity card featuring a digital certificate that, together with a PIN code, can also be used for online authentication of citizens, see Alvarez et al. 2009, p. 499.

[51] Art. 27a-27d.

[52] Art. 27d.

[53] Art. 27e-27k, Art. 27m.

[54] Art. 27l.

the e-voting system.[55] Finally, the Federal Council is authorized to collect data on the usage of e-voting systems and commission research in this area.[56]

The majority of these provisions are aimed at ensuring free and secret suffrage (Braun 2004). The following brief summary of some of the requirements outlined in the Ordinance might give some sense of the ways in which legal, technical, and organizational measures need to play in concert in order to ensure the basic principles mentioned in the previous paragraph.

(a) Free Suffrage

The provisions that seek to guarantee free suffrage include a number of design requirements for the e-voting user interface and application, a series of mandatory information and notification requirements, and requirements regarding the integrity of data during the transmission process.

User interface and application design: The user interface has to be built in such a way so that it does not encourage voters to vote precipitately or without reflection.[57] Manipulative pop-up messages are not permitted.[58] Further, the application must allow users to change their choices at any time before submitting their vote electronically or terminating the voting procedure.[59] The design of the user interface has to take into account the special needs of voters with handicaps.[60]

- Mandatory information and notifications: Users of the e-voting system must be informed prior to the submission of their vote that they are participating in an authentic ballot through electronic means; they have to confirm this message.[61] The transmission of the vote needs to be transparent for the voter.[62]
- Integrity of data: Information has to be provided that allows voters to check the authenticity of both, the website and the servers used for e-voting.[63] Any data has to be transmitted in an encrypted form that precludes altered voting data from being counted.[64]

(b) Secret suffrage

The Ordinance specifies a series of detailed requirements in order to ensure secret suffrage in the e-voting environment. It requires that all appropriate measures be taken in order to ensure that no connection can be drawn at any

[55] Art. 27k, Art. 27m and Art. 27nbis.

[56] Art. 27o.

[57] Art. 27e subpara 1.

[58] Art. 27e subpara 4.

[59] Art. 27e subpara 5.

[60] Art. 27ebis.

[61] Art. 27e subpara 2 and subpara 3.

[62] Art. 27e subpara 6.

[63] Art. 27e subpara 8.

[64] Art. 27e subpara 7.

time between a vote and a voter.[65] This principle is concretized through a series of partly overlapping and partly complementary procedural/organizational and technical requirements. Among them are the following[66]:

- Procedural/organizational safeguards: Transmission channels, authentication systems, registration processes, and the act of casting the vote need to be organized in such a way that no connections can be drawn between an act of voting and a voter.[67] Separation of any data processing operations in connection with e-voting from all other activities[68]; the opening of the electronic ballot box or one of its parts needs to be carried out by at least two people, needs to be documented and be open to review on the part of the voting authorities.[69] Measures need to be taken in order to make sure that no information required in the context of data processing can be misused to violate the secrecy of the vote.[70] Moreover, submitted votes need to be sorted in an anonymous form and need to be organized in such a way that no conclusions can be drawn with regard to the sequence by which the votes were submitted.[71]
- Technical requirements: Measures need to be taken to prevent any authorized and unnecessary access to the e-voting server infrastructure and/or the electronic ballot.[72] Encryption is required throughout the entire voting process, starting with the encryption of the vote prior to its submission, including the encryption of the transmission process and ending with the encrypted storage of the votes.[73] The votes shall be decrypted only at the time when they are to be counted.[74] The e-voting client must enable users to delete the vote from the voting device upon transmission,[75] and the vote must disappear from the screen of the voting device used by the voter as soon as the vote has been submitted; the e-voting software has to make it impossible to print a copy of the submitted vote.[76]

---

[65] Art. 27g subpara 1 and Art. 27f subpara 1.

[66] See also Braun 2004, p. 48 for an overview.

[67] Art. 27f subpara 2. See also Art. 27f subpara 4, which requires that voter verification be anonymous, but designed in a way that ensures that the voting authority can ensure the one person—one vote principle.

[68] Art. 27g subpara 2.

[69] Art. 27g subpara 3.

[70] Art. 17g subpara 4.

[71] Art. 27h subpara 2.

[72] Art. 27h subpara 1.

[73] Art. 27f subpara 3.

[74] Art. 27f subpara 5.

[75] Art. 27h subpara 3.

[76] Art. 27h subpara 4.

In addition to these provisions at the federal level, the cantons that are introducing or already operating an e-voting system have amended their respective cantonal laws governing the exercise of political rights. Usually, however, the amendments of the cantonal laws are less fine-grained than the provisions summarized here. Another set of legal provisions—in the form of an agreement among the involved cantons and the Swiss Confederation—deals with the use of the e-voting infrastructure 'borrowed' from one canton by another (with Basel-Stadt being the first case in a series of expected e-voting 'outsourcing' solutions.) Such an agreement specifies, inter alia, how the cantons should cooperate in order to get the permission of the Federal Council for the project, which voters will be permitted to use the e-voting system, how voters will be authenticated and verified, what data format and data standards must be used for data transmission between the cantons, and what the production and distribution of voting materials shall look like. It also addresses issues such as hotline services, security measures, information policies, risk management, time windows for the availability of e-voting, analysis of votes, audits, cost-splitting, etc.[77]

7.4.2.2 System Design

As of January 2010, three different systems for e-voting are in use in Switzerland that operate within the legal framework and the specifications outlined in the previous paragraphs. All of them are cloud applications, i.e., the only software that a voter needs to use the system is a web browser.[78] While Geneva, Neuchatel, and Zurich each have developed different solutions, Basel-Stadt decided to use Geneva's platform to provide e-voting to Swiss living abroad. Before looking at some basic characteristics of the voting systems, one has to note that the current technological and organizational architectures are not static, but will be further improved upon over time as technology progresses and as issues or problems with the actual operation of the systems emerge.

So far, the experiences have been mostly positive. In particular, there have been no reports of fraud or major system failures. However, interoperability issues have surfaced: The Geneva system did not work properly for all Mac users in the November 2008 vote due to a Mac operating system upgrade that was released just days before the poll. This glitch resulted in an estimated 'three to four point of

[77] See, e.g., Übereinkunft zwischen dem Kanton Basel-Stadt und dem Kanton Genf sowie der Schweizerischen Eidgenossenschaft über die Beherbergung von Auslandschweizer Stimmberechtigten des Kantons Basel-Stadt anlässlich eidgenössischer Urnengänge auf dem Vote électronique-System des Kantons Genf [Treaty between the canton Basel-Stadt, the canton Geneva, and the Swiss Federation on hosting the Swiss abroad registered in Basel-Stadt on the e-voting system of Geneva for federal ballots].

[78] Via the web browser, a digitally signed applet is subsequently loaded after navigating to the voting platform, see Rota 2008, slide 8.

online turnout' lost 'for technical reasons.'[79] But Mac users were not the only ones to encounter difficulties: after the release of Windows XP, service pack 2, which used to block pop-up windows in browsers by default, some users were prevented from casting their vote online in the polls of September and November 2004.[80] Somewhat less severe and easier to remedy was the fact that voters in Zurich were not able to vote online using the latest version of the popular web browser 'Firefox.'[81] The lack of an open-source approach or rather the proprietary nature of the Geneva system, which was developed with the help of Hewlett-Packard and Wisekey among others, was also one of the main points of critique.[82]

At the core of the three e-voting systems are mechanisms that provide the three basic functionalities of any voting process: (a) authentication of the user, (b) vote and confirmation, and (c) registration and counting of the vote.

(a) Authentication

E-voting in its current incarnation starts with snail mail. A couple of weeks before the vote, the registered voters in each canton receive official documents in the mail. The materials include a voting card in the case of Geneva and Zurich,[83] which contain authentication information in the form of a number or user-ID that is valid for the upcoming ballot only.

The Neuchatel system is different as it relies on previous authorization such as, is used in e-banking systems. In order to use the e-voting system, citizens have to register with the authorities by signing a form in advance to get access to the 'Guichet Unique.' Once the authorities have set up a user account for them, the citizens receive their password and login data in the mail. This login data is not only valid for the upcoming ballot but grants access to the 'Guichet Unique' at all times. Upon authentication with the card number or login data, respectively, the voter is connected to a secure server and presented with the ballot.

Notably, alternative mechanisms of authentication have been considered by the designers of cantonal voting systems, but rejected for one reason or another. Using social security numbers or other personal identification information—or even relying on biometrical data (Morales-Rocha et al. 2008)—may make the system more robust in one way or another, but raises serious privacy concerns. The use of digital signatures is not common yet, but may be an option for voter authentication in the future (Braun and Brändli 2006) and has actually been the key enabler of nation-wide e-voting in Estonia (Alvarez et al. 2009).

---

[79] See http://www.geneve.ch/evoting/english/historique.asp

[80] Ibid.

[81] Neue Züricher Zeitung 2009.

[82] This critique was prominently expressed by the Linux user-group called 'Gull.' See a german translation of an open letter addressed at the State Council of Geneva at http://www.ch-open.ch/html/oss/evoting.html

[83] See http://www.ge.ch/evoting/carte-de-vote.asp and https://evoting.zh.ch/MainPage/pdf/anleitung_evoting.pdf respectively.

(b) The vote and confirmation
A symbol serving as a fingerprint or a control code on the voting card allows users to verify that they have navigated to the official voting website and are securely connected. When the voter has marked her choice, the system provides a recapitulation of the choices made and asks to be confirmed. The voter then has to verify her identity. Here the systems of Geneva and Zurich differ from the one in Neuchatel: citizens of the former cantons need to enter their birth date and the pin code printed on their voting card. The pin code is hidden by a rubber seal, which can be scratched off the paper. Once the rubber seal is removed, the voting card is invalidated and can only be used for a vote by mail or at the ballot box if the voter has not cast their vote electronically.[84] The Neuchatel system, in contrast, asks for personal validation and confirmation codes that have been sent out to the users of the 'Guichet Unique' with the voting information.[85]
When the voter's identity is successfully verified, the vote can be submitted. After submission, voters receive a confirmation that their vote was accepted and recorded by the system (Geneva) or a message that confirms the vote (Zurich and Neuchatel). The time window for voting online lasts from the moment the voting card is received in the mail (usually three weeks prior to the vote) until midday on Saturday before polling stations open on Sunday (Bosshard et al. 2008).

(c) Registration and counting of votes
As a next step in the process, the encrypted vote is sent from the voter's computer to the servers of the respective e-voting platforms, which are protected by firewalls and other technologies (Knöri 2006). Cast votes are saved in a database (an 'e-ballot box') in encrypted form and—in the case of Zurich—simultaneously saved on a Write Once Read Multiple (WORM) medium in order to provide an additional layer of security and data integrity (Knöri and Prader 2006). When a vote has been registered, the authorization to vote (in the same ballot) is immediately cancelled in the database (Braun and Brändli 2006).

The opening of the 'e-ballot box' happens in the presence of inspectors or controllers, who are appointed by the Cantonal Government.[86] The members of this electoral board enter their encryption keys which allow the system to process the votes. This is not only intended to provide privacy and security, but the involvement of inspectors in sensitive processes has been interpreted as a way of generating trust

[84] See http://www.geneve.ch/evoting/english/securite.asp and https://evoting.zh.ch/MainPage/pdf/anleitung_evoting.pdf

[85] See http://www.bk.admin.ch/themen/pore/evoting/00774/00781/index.html?lang=de

[86] In Geneva, these controllers are nominated by political parties. See http://www.geneve.ch/evoting/english/securite.asp

in and increasing the legitimacy of e-voting which otherwise would be an entirely automated procedure.[87] Without ever linking them to the voter,[88] the system then adds the calculated number of electronic votes to the results from the count of physical voting cards that have been submitted by mail or at the polling station.

While there is a centralized voter registry in Geneva, voter registration data in Zurich is only transferred from the individual communities in order to generate the registration letters and verify voter identification upon using the e-voting system (Knöri and Prader 2006). Thus, a 'virtual' registry is generated anew for each voting occasion, but is then deleted immediately thereafter (Knöri and Prader 2006). Somewhat like the Zurich system, the canton of Neuchatel establishes a new virtual voters' registry on each polling day by collecting updated information from all municipalities' registries.

7.4.2.3 Social Norms

The act of exercising political rights through voting is not only governed by the legal, technical, and organizational arrangements, but also shaped by social norms. These norms, in turn, interact with technological and institutional innovations as Swiss history impressively demonstrates. In order to anticipate the promise, but also limits of new voting techniques such as e-voting, it is important to understand these interactions and evolutionary mechanisms. The move from public to private voting in Switzerland is illustrative in this context.

Historically, voting in Switzerland was conceived and practiced as a public act. Even today, two cantons—Appenzell Innerrhoden and Glarus—still follow the tradition of public voting at open-air assemblies (so-called 'Landsgemeinde'), where the citizens gather at a public place and vote on issues to be decided by raising their arm (Helg 2007). The first step away from public voting was the practice of casting votes at polling stations, through which the expression of opinion became a private act. Nevertheless, the public space still played and continues to play an important symbolic role by bringing citizens together and creating a sense of community and self-governance. The second and perhaps even more dramatic step in the process from public to private voting occurred in 1994, when federal law mandated that the cantons provide postal voting for all citizens (since 1966, postal voting had been allowed for people who were not able to go to polling stations) (Braun 2006).

In the context of this paper, several aspects that accompanied the shift from public to private voting are of interest. First, it is important to understand that the concept of secret suffrage, which plays such a prominent role in e-voting, is a rather recent innovation in historic terms. The notion that democracy and the secrecy of the vote should be inseparable was only developed at the beginning of

[87] Braun and Brändli 2006, p. 34.

[88] This is achieved by using a mixing or shuffling protocol. See Cervelló 2009, p. 5.

the 20th century.[89] In fact, secret voting was considered to be 'characterless,' while public voting was thought to make people (quite literally) stand up for their beliefs (Helg 2007). It can only be speculated as to what extent the Swiss tradition of public voting still influences our attitudes when it comes to the importance of voting secrecy and how, for instance, this attitude might affect the adoption rate of e-voting systems.

Second, it is interesting to recall the reservations that were expressed when postal voting was considered as a new voting technique. Two proposals by the Federal Government to introduce postal voting prior to 1994 had been dismissed by the parliament in 1936 and 1947 because of the fear of manipulation. Transparency and the presence of others at the Landsgemeinde, but to a lesser extent also at the polling stations, had been seen as effective mechanisms of social control that had also minimized the risk of manipulation (Helg 2007). Viewed from this historical angle, it hardly comes as a surprise that e-voting with its radical privatization and lack of transparency of the act and process of voting has caused concerns in this respect, as discussed above.

The third observation relates to the malleability of norms. When cantons finally did introduce postal voting, this new possibility to conveniently cast a ballot without going to the polling station was hugely popular. Only four years after introduction, 44% of all votes were sent in by mail.[90] The Swiss quickly started to appreciate the convenience factor, accepted the increase of privacy of the vote as well as the increased risk of manipulation that comes with it. Admittedly, this observation might be more accurate for urban areas than for rural regions, where people still appreciate the social aspect of meeting at the polling stations.[91] In fact, especially in small municipalities social signaling seems to be an important aspect that should not be underestimated: Turnout has decreased in small municipalities of the canton Zurich after postal voting was introduced and the signaling effect of voting was reduced (Funk 2005).

Against this historical background, it will be interesting to see how the norms of voting will interact and further evolve when e-voting becomes more available across Switzerland and for Swiss citizens living abroad. Doubtlessly, e-voting will move the act and process of voting even more consequently away from the public sphere and into the privacy of homes. At the same time, the complexity of the voting system increases once again, and for most people the procedure becomes less transparent. Past experience demonstrates how such knowledge gaps are compensated by socially generated trust in experts, socio-technical systems, and relatively few instances where trust has been disappointed (Burkert 2009). Consequently, it can be expected that the trust in the institutions of voting as it has evolved over time and across technologies (Landsgemeinde, polling stations, postal voting) may also be projected on e-voting systems, reinforced by the high levels of

[89] For an overview of political theories and arguments for and against public voting, see Buchstein 2000.

[90] Federal Chancellery (b), p. 2.

[91] The densely populated cantons of Geneva and Basel-Stadt have a much higher percentage of votes sent in by mail than rural Appenzell-Innerrhoden or Glarus. Federal Chancellery (b), p. 3.

trust in information and communication technology more generally.[92] The institutional framework outlined above, safeguards these expectations, but also defines the limits of trust as a compensation mechanism by marking the boundaries of the new technology and limiting the possible negative consequences that are associated with it when things unexpectedly go wrong. The institutional framing of e-voting as a supplementary technique and the cap on online participation mentioned above are perhaps the most illustrative examples of this sort (Burkert 2009).

7.5 Conclusion

While the idea of using the Internet for voting seems rather straightforward in a time in which the first generation of children 'born digital'—who cannot imagine a life without Google or Wikipedia—enters the workforce (Palfrey and Gasser 2008) and even many of their parents make flight reservations online or use e-banking services, the Swiss experience illustrates some of the challenging complexities associated with the introduction and operation of e-voting systems. These complexities are manifold and include legal, technological, political, and social challenges at different levels of the political ecosystem.

A closer analysis of the problems associated with e-voting—including concerns regarding security and manipulation—suggests, however, that only a small subset of the issues currently up for discussion is really new. Previous innovations in voting techniques including the casting of votes at polling stations and, in particular, postal voting have triggered concerns similar to those discussed today in the e-voting context. Viewed from that angle, it seems that at least some of the challenges associated with the new ways in which the highly symbolic act of voting can be exercised in the digital age have simply become more explicit and visible in the e-context. While many of the risks and challenges might not be qualitatively new, they might be distinct with regard to their potential scale. For instance, the specter of computer-based large-scale data manipulation does indeed seem more troublesome than the potential of relatively limited, high-cost manipulation of the postal voting system.

The possible downsides of Internet voting, of course, need to be taken very seriously. But the Swiss example also illustrates some of the important promise associated with e-voting, particularly in terms of increased autonomy and, potentially, enhanced participation and quality. It shows how the various forces—legal, technological, political, and cultural—can actually be used and orchestrated in order to address some of the key challenges, while creating a more advanced and richer ecosystem for voting. As such, its approach might at least be a source of inspiration for other countries.

Acknowledgments The authors are grateful to Herbert Burkert, John Palfrey, and James Thurman for conversations and comments.

[92] For example, according to the poll 'Baromédia 2002,' 53% trust in the Internet as media (compared to 65% who trust in banks and churches). Cited in Bonard 2003, p. 31.

References

Alvarez MR et al (2009) Internet voting in comparative perspective: the case of Estonia. PS: Polit Sci Polit 42(3):497–505

Berkman Center (2009) Next Generation Connectivity: a review of broadband Internet transitions and policy from around the world. http://www.fcc.gov/stage/pdf/Berkman_Center_Broadband_Study_13Oct09.pdf

Bonard C (2003) Chances et défis du vote par Internet. In: Journées 2002 d'Informatique Juridique Berne, pp 29–57

Bosshard F et al (2008) E-Voting im Kanton Zürich: 'Abstimmen per Internet—Risiko oder Komfort?' [E-voting in the canton of Zurich: Voting via the Internet—risk or convenience?]. Presentation held in Zurich on 20 October 2008

Braun N (2004) E-Voting: Switzerland's projects and their legal framework–in a European context. In: Prosser A, Krimmer R (eds) Electronic Voting in Europe: Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, pp 43–52

Braun N (2006) Stimmgeheimnis [Secrecy of vote]. Stämpfli, Berne

Braun N, Brändli D (2006) Swiss e-voting pilot projects: evaluation, situation analysis and how to proceed. In: Krimmer R (ed) Electronic Voting 2006. Gesellschaft für Informatik, Bonn, pp 27–36

Buchstein H (2000) Öffentliche und geheime Stimmabgabe [Public and secret voting]. Nomos, Baden-Baden

Burkert H (2009) Das 'Wahlcomputer'-Urteil und E-Voting. Digma 9:112–117

Cervelló G (2009) The e-participation project of Neuchâtel. European Journal of ePractice 7:5. http://www.epractice.eu/en/document/287937

Chevallier M et al (2006) Success factors of Geneva's e-voting system. Electron J e-Gov 4(2):55–62

Eicholzer H (2006) eVoting—Erfahrungen der Gemeinde Bertschikon—Ein Projektbericht [e-voting—experiences of the municipality of Bertschikon]. http://www.sgvw.ch/d/fokus/Seiten/070306_evoting_eichholzer.aspx

Engi L, Hungerbühler F (2006) E-Voting–Stand und Entwicklung in der Schweiz [E-voting–status quo and developments in Switzerland]. Medialex 1:17–27

Federal Chancellery (a) Synoptische Darstellung der Schweizer Vote électronique Versuche in den Jahren 2003 bis 2007 [Overview of e-voting pilot-projects from 2003 to 2007]. http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de&download=M3wBPgDB_8ull6Du36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIR8gX9_bKbXrZ6lhuDZz8mMps2gpKfo

Federal Chancellery (b) Umfrage über die briefliche Stimmabgabe [Survey on postal voting]. http://www.bk.admin.ch/dokumentation/publikationen/00284/02032/index.html?lang=de&download=M3wBPgDB_8ull6Du36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN4e3p8bKbXrZ6lhuDZz8mMps2gpKfo

Federal Council (2002) Bericht über den Vote Électronique. Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte vom 9. Januar 2002 [Report on e-voting. Opportunities, risks and feasibility of the exercice of political rights by electronic means]. Federal Gazette 645

Federal Council (2006a) Bericht über die Pilotprojekte zum Vote électronique vom 31. Mai 2006 [Report on the e-voting pilot-projects]. Federal Gazette 5459

Federal Council (2006b) Botschaft über die Einführung der allgemeinen Volksinitiative und über weitere Änderungen der Bundesgesetzgebung über die politischen Rechte vom 31. Mai 2006 [Dispatch on the introduction of a general people's initiative and on further amendments of Federal legislation on political rights]. Federal Gazette 5261

Federal Council (2009a) Arrêté du Conseil federal autorisant un essai de vote électronique dans le canton de Neuchâtel lors de la votation populaire fédérale du 17 mai 2009 [Decision of the Federal Council on the approval of an e-voting test in the canton of Neuchatel on the occasion

of the Federal ballot of 17 May 2009], Federal Gazette 2009 1161 and Arrêté du Conseil federal autorisant un essai de vote électronique dans le canton de Neuchâtel lors de la votation populaire fédérale du 27 septembre 2009 [Decision of the Federal Council on the approval of an e-voting test in the canton of Neuchatel on the occasion of the Federal ballot of 27 September 2009], Federal Gazette 2009 4617

Federal Council (2009b) Bundesratsbeschluss über die Zulassung eines Versuchs zu Vote électronique im Kanton Neuenburg im Rahmen der eidgenössischen Volksabstimmung vom 29. November 2009 [Decision of the Federal Council on the approval of an e-voting test in the canton of Neuchatel on the occasion of the Federal ballot of 29 November 2009]. Federal Gazette 2009 7013

Franklin MN (2004) Voter turnout and the dynamics of electoral competition in established democracies since 1945. Cambridge University Press, Cambridge

Funk P (2005) Theory and evidence on the role of social norms in voting. http://ssrn.com/abstract=627347, p 6

Geser H (2002) E-voting Projects in Switzerland. In: Sociology in Switzerland: towards cybersociety and vireal social relations. http://socio.ch/intcom/t_hgeser12.htm

Gfs.bern (2005) Das Potenzial der elektronischen Stimmabgabe [The potential of electronic voting]. Berne 2005. http://www.gfsbern.ch/pub/vote-electronique.pdf

Government Council, Canton of Zurich (2007) E-Voting wird im Jahr 2008 weitergeführt—weitere Gemeinden und Stadtkreise werden zugelassen [E-voting will be continued in 2008—more municipalities and city districts will be admitted]. Press Release, 4 October 2007. http://www.ji.zh.ch/internet/ji/de/aktuelles/medienmitteilungen/aktuelle_news/evoting_2008.html

Helg F (2007) Die schweizerischen Landsgemeinden [The public open-air essamblies of Switzerland]. Schulthess, Zürich

Imhof I (2006) Schritt für Schritt zum 'Vote électronique' [Step by step towards e-voting]. Neue Zürcher Zeitung, 13 September. http://www.nzz.ch/nachrichten/zuerich/article9zhm5_1.333163.html

Knöri D (2006) E-Voting und dessen Herausforderung [E-voting and its challenges]. Presentation held at Telematiktage Bern. On file with authors

Knöri D, Prader E (2006) E-Voting des Kantons Zürich [The e-voting system of the canton of Zurich]. 10 February. On file with authors

Linder W (2003) E-Voting–Eine Belebung der direkten Demokratie? LeGes 1:103–124

Morales-Rocha V et al (2008) Secure remote voter registration. In: Krimmer R, Grimm R (eds) Electronic Voting 2008. Gesellschaft für Informatik, Bonn, pp 95–108

Neue Züricher Zeitung (2009) Stimmabgabe über 'Firefox'-Browser nicht möglich [Voting with 'Firefox' browser not possible]. 23 November. http://www.nzz.ch/nachrichten/zuerich/stimmabgabe_browser_1.4054104.html

Oppliger R (2008) Sicherheit beim E-Voting. E-Voting auf unsicheren Client-Plattformen. Digma 8:82–85

Palfrey J, Gasser U (2008) Born digital. Basic, New York

Prader E (2006) Das e-Voting System im Einsatz [The e-voting system in use]. Presentation held at Telematiktage Bern 2006, slides 24–25. On file with authors

Rota D (2008) E-government and Electronic Voting. Presentation held at the Council of Europe's Future of Democracy Forum, 15–17 October 2008, Madrid, p 17. http://www.coe.int/t/dgap/democracy/Source/Democracy%20Forum/2008/Presentations/Rota_Presentation_FFD08.pdf

Strategy of the Federal Council for an Information Society in Switzerland (1998) 18 February 1998. http://www.bakom.ch/themen/infosociety/00695/index.html?lang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCDdH95gWym162epYbg2c_JjKbNoKSn6A

Strategy of the Federal Council for an Information Society in Switzerland (2006) January 2006. http://www.bakom.ch/themen/infosociety/00695/index.html?lang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCDdX95e2ym162epYbg2c_JjKbNoKSn6A

Trechsel A (2007) E-voting and electoral participation. In: de Vreese C (ed) Dynamics of Referendum Campaigns–An International Perspective. Palgrave, London, pp 159–183

Chapter 8
Striving Behind the Shadow: The Dawn of Spanish Politics 2.0

Ismael Peña-López

Abbreviations

ICT	Information and Communication Technology
RSS	Really Simple Syndication
PSOE	Partido Socialista Obrero Español

Contents

8.1 Introduction 130
8.2 A Definition of 'Politics 2.0' 131
8.3 The Spanish e-Readiness Level and Web 2.0 132
8.4 Spanish Online Politics 133
8.4.1 An Introduction to Online Politics 133
8.4.2 Spanish Parties and Online Politics 134
8.5 Political Blogging 137
8.6 Campaigning 138
8.7 Some Practical Examples to Pave Future Ways 140
8.7.1 The Power of Cyberactivism 141
8.7.2 The Acknowledgment and Naturalization of Cyberactivism 141
8.7.3 Blogging to Build and Weaved Blogging 142
8.7.4 Open Government, Open Parliaments 143
8.8 Conclusion 143
References 145

Contribution received in 2010.

I. Peña-López (✉)
School of Law and Political Science of Open University of Catalonia (UOC), Barcelona, Spain
e-mail: ipena@uoc.edu

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_8,

8.1 Introduction

As in everywhere else in the World, the Spanish awakening to Politics 2.0 has been overwhelmingly influenced by US Politics. Spanish politics was awakened to web politics after Howard Dean's campaign to the 2004 presidential candidacy, where blogging and other online services like Meetup became important tools for campaigning. The US President Barack Obama's long path to the presidency—from February 2007 when he announced his candidacy for the presidency of the United States, until he assumed office in January 2009, after 2 years of primary and presidential elections—where the Internet was a crucial factor of success, draw the blueprint that many are trying to understand and replicate.

At the domestic level, we would like to remind the reader that the government of the Spanish Prime Minister José María Aznar (1996–2004) is seen by many as a turning point in Spanish politics. On the one hand, his coming into power implied the end of the Spanish Transition, which many date from the death of the dictator Francisco Franco (1975) until the defeat of the Prime Minister Felipe Gonzalez's Socialist Party in 1996.[1] On the other hand, it is just after Mr. Aznar that the Internet—and Information and Communication Technologies (ICT) in general—comes under the spotlight of the political scenario: first, in the 2004 election that the Partido Popular lost in favor of Mr. Rodríguez Zaptero's socialist party and then in the 2008 election, where Rodríguez Zapatero was re-elected.

It is in this framework of international influence combined with an endogenous change that Politics 2.0 rise in Spain. The first decade of the 2000s is not only the one where ICTs see them being adopted massively, but also an age of political change at all levels after the political hinge of Mr. Aznar's mandate. But, despite the fact that the storm was perfect—or maybe just because of that—Spanish Politics 2.0 are way behind the forecasts of the Web 2.0 pundits and digerati. Spanish Politics are nearer to being 1.5 than 2.0, seem to be reinforcing the status quo and the political parties' plutocracy and, at its best, are more focussed on a shallow debate about the forms rather than a deep wish to transform the agora.

In this chapter we will bring some evidence to back the previous statement. First, we will bring a rough picture of the state of adoption of ICTs and the Web 2.0 in Spain. Then, we will focus on what is happening at the debate—or the deliberation—level, especially in the Spanish political blogosphere—understanding political as professional politicians and non professionals talking about politics. Lastly, the focus will shift from the debate to campaigning and political elections. Some discussion and conclusions will close the chapter.

[1] Though there are many opinions on when did the Spanish Transition end—the approval of the 1978 Constitution, the socialist party winning the 1982 elections, et cetera—there is full acknowledgement in considering Mr. Aznar as the first president belonging to the new generation of politicians that were not part of the Dictator's governments or fought against them.

8.2 A Definition of 'Politics 2.0'

In 2005, Tim O'Reilly published a seminal article (O'Reilly 2005) in which he provided a definition for the term Web 2.0, which had gained a huge momentum during the previous year since the first edition of the Web 2.0 Conference in October 2004.

The concept gathered both technological and philosophical (in the sense of behaviors and attitudes) issues. At the technological level, it dealt with the importance of the web as a delivery (of content and services) platform by excellence; data as the core component of all kinds of communications and interchanges; software as a service and not a product, then becoming more important, access to software than its 'physical' purchase; predominance to RSS and associated procedures for the exchange of content; or (while keeping the importance of the web as a platform) the need to create technologies that were portable across devices. At the philosophical level, it dealt with both cause and consequence of the technological advances, the spread (and enabling) of a contribution and participation culture by the society at large (and not only by institutions or organized associations); the acknowledgement that anyone could actually contribute with their knowledge and opinion (the 'wisdom of crowds'); the raise of a culture of mixing, assembling and aggregating content; and the will to have rich user experiences when interacting online (vs. passive, unidirectional, monotonous approach which had been common ground in the previous years).

Besides the 'formal' definition of the Web 2.0, it has more often been described through some tools and the new and, characteristic ways of using them: blog and nanoblog, wiki, social bookmarking, photo and video sharing websites, tagging and 'folksonomies,' syndication and aggregation, etc.

After this philosophical approach—boosted by the technological advancements—many have adapted some of the core definitions to many aspects of life. Thus, for instance, Education 2.0 is often referred to as a shift from unidirectional lecturing towards a more participatory approach of learning, based in collaboratively creating learning materials, an intensive usage of Web 2.0 tools, or openness and sharing of the process of learning, just to name a few. And along with education, we can find debates around Research 2.0, Culture 2.0, Government 2.0, Journalism 2.0, Enterprise 2.0, and Politics 2.0.

Our own understanding of Politics 2.0, and the one that we will be using as a definition to frame this chapter, is composed by the following characteristics:

- Ideas: not closed and packaged propaganda. Ideas that can be spread, shared and transformed by members of the party and partisans, sympathizers and supporters, and the society at large;
- Open data: ideas are backed by incredible amounts of data and information made openly available to the general public, and most time provided with open licenses that allow their reuse and remix;

- Participation: of all and every kind of people and institutions, blurring the edges of the 'structures' and permeating the walls of institutions, making communication more horizontal and plural;
- Loss of control of the emission of the message, that now can be transferred outside of mainstream media and diffused on a peer-to-peer and many-to-many basis by means of Web 2.0 tools;
- Loss of control of the creation itself of the message: being data and participation available, Web 2.0 tools at anyone's reach, and with minimum digital competences, the message can even be created and spread bottom up;
- Acknowledgement, hence, of the citizen as someone who can be trusted (and used) as a one-man think-tank and a one-man communication-media;
- Reversely, possibility to reach each and every opinion, target personal individuals with customized messages, by means of rich data and web 2.0 tools, thus accessing a long tail of voters that are far from the median voter;
- Construction of an ideology, building of a discourse, setting up goals, campaigning, and government become a continuum that feedbacks in real time.

We admit that this is neither a usual or a formal description, nor a comprehensive set of characteristics. We believe, though, that it will serve in providing a framework for what is intended to explain in this chapter.

8.3 The Spanish e-Readiness Level and Web 2.0

Before speaking about the state of Spanish online politics, we thought we should bring a quick overview of the state of e-Readiness of Spain.

Concerning its stage of digital development, Spain is a digital striver (Peña-López 2009b). This means that the economy is following the same path that the most digitally advanced economies are setting, but lags behind in the performance of most digital indicators: ICT infrastructures, the ICT sector, digital literacy and competences, the legal and regulatory framework, and the existence and usage of digital content, and services.

Despite the fact that the pervasiveness of mobile phones, computers, and Internet is near the European average in Spain (115.3% mobile penetration, 63.6% of homes having a computer, 51.0% with Internet access),[2] the effective usage of the Internet—arguably the main indicator to look at when talking about Politics 2.0—is still low or, to say the least, suboptimal. 61.7% of the population answered in the third quarter of 2008 that they had 'ever used the Internet' and just 46.3% of the total users were intensive users—that is 28.6% of the total population had used the Internet 'the previous week.'

[2] All data in this section, if not stated otherwise, are from Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información 2009.

The socio-economic profile of the Internet users is similar to the one we find in higher income countries:

- Slight unbalance towards males, but decreasing;
- Higher ratio of users among the younger, the segment of the population, reaching really low ratios amongst elderly people;
- Predominance of middle and high classes;
- Predominance of educated people, with secondary or higher education degrees;
- No formal training on Internet issues, but users are either self-taught or learnt with the help of family, friends and/or colleagues.

Concerning more '2.0' indicators, findings are quite self-explanatory.

On the one hand, 75% of Internet users accessed social networking sites and had profiles in them and participated—with different intensities—in these virtual spaces. On the other hand, just 21.4% of the intensive Internet users (people that used the internet in the previous week) read blogs and only 7.9% of the intensive Internet users wrote on their (or on third parties') blog.

These two last indicators, along with others about usage (online shopping, access to e-administration sites, e-learning activities, etc.) profile a Spanish Internet user that mainly access the Internet for leisure and, on a second stage, for information gathering and learning activities. In general, it is a user that just seldom contributes or creates user generated content.

The Spanish Web 2.0 is populated by a smallest group of prosumers on the top of an iceberg. The greater mass of this group is invisible, accesses the Internet on a random basis or does it in the quest of leisure alternatives. In general, though, Spanish Internet users do not periodically participate in what it is at stake in this chapter: politics.

So, what is really happening in online politics, both in terms of 'Web 1.0' and Web 2.0?

8.4 Spanish Online Politics

8.4.1 An Introduction to Online Politics

Online politics have evolved in width and depth since Internet access was made public in late 1994 and early 1995.

The first years of the Internet can be described as an information and participation sandbox, where citizens checked whether this could be a new place where to get better and personalized information about politics, and to interact amongst them (Jacobson 1999; Katz et al. 2001; Sunstein 2001).

But the then unidirectionality of the Internet made it to be conquered as a political tool by political parties (Bimber and Davis 2003), being used for what still today is the king use of online politics: online campaigning. There is quite a

major consensus that US Politics have been the laboratory where the Internet has been put into work for political campaigning. Howard Dean's campaign during the primary elections for the 2004 presidential candidacy is acknowledged to be the first one in which the Internet had an important role (Cornfield 2005). Maturity—at least in today's standards—came during both primary and presidential elections; by the then candidate Barack Obama in 2008 (Pew Research Center for The People & The Press 2008; Smith and Rainie 2008).

The lion's head of online politics, online campaigning has caught the attention of researchers to analyze both what happens during elections (Hillygus and Shields 2007) or after them (Smith 2008).

Related to campaigning, the implication of partisans and the citizenry at large has increasingly been put under the spotlight, especially due to the popularization of blogging in general and, specifically, for political issues (Elmer et al. 2009; Criado and Martínez Fuentes 2009). Blogging has, of course, had also an impact on how people face mainstream media. Thus, the always difficult relationship between political parties (as message creators and senders), media (as mediators) and citizens (as receivers, but now also as senders and re-senders) has been also analyzed in parallel in and out of campaigns (Howard 2005; Dutton 2007; Gibson 2009; Cristancho and Salcedo 2009).

Besides campaigning, some incipient interest has been put too in e-democracy and the creation of debate and opinion, prior or collateral to campaigns (Noveck 2005; Davies and Peña Gangadharan 2009), citizen activism (Norris and Curtice 2006) or even control and repression (Morozov 2009).

In general, almost all—if not all—the aspects of politics, political engagement and citizen participation have been permeated by the Internet and life online (Chadwick and Howard 2008; Oates et al. 2006; Chadwick 2009; Fleishman-Hillard 2009), being the US usually at the head of experimentation and implementation, and the rest of the world at shorter or larger distances from these two countries.

In this landscape, where does Spain fit?

8.4.2 Spanish Parties and Online Politics

In general, the statements made by Borge (2005) still apply. Acknowledging that generalizations are also rough approximations to reality, and being aware that other behaviors exist and exceptions apply, in general, political parties in Spain mainly use websites and the Internet at large to broadcast their own messages, and, as broadcasters, have little purpose in engaging in a two-way communication with their partisans or their (potential) voters. Hence, there is a lack of agora where to deliberate and usage of the Internet is at the lower steps of Arnstein's (1969) ladder of participation. The trend—triggered overall by the US politics example, an always present mirror for Spaniards in the matter—is to move beyond this ancient approach to online politics, and there already exists some momentum in this line, as we will be seeing later on.

When looking at the reasons behind this scenario, two major reasons seem to arise, the former quite naturally, the second one not that intuitive. On the one hand, we have already described the state of e-Readiness in Spain. Indeed, in relative terms, Spain lags—and has always lagged—behind the US in matters of e-readiness, as a quick comparison between Kirkman et al. (2002) and Dutta and Mia (2009) will also clearly show. It is, thus, not bold to assume that this e-readiness lag has had a negative impact in Spanish online politics lag. On the other hand, it also seems (Jensen 2009) that the low levels of political participation in Spain might also be caused because of high levels of Spaniards trust in institutions: hence, the Internet would still be used in a vertical, institutional way, despite its possibilities to be used otherwise, in more horizontal and participative way, as there would not be a need for it, being institutions (political parties, governments) regarded as trustful and convenient actors for politics.

This second reason would explain this lack of participation despite the fact that the Spanish web has been found to have a certain bias towards the left wing (Robles 2008), which has historically been more participative-prone than the right wing.

In this sense, Batlle et al. (2007) also found, when analyzing Catalan parties,[3] that left-wing parties showed not higher degrees of participation or collective decision-taking online than their right-wing counterparts. Indeed, the typology of the party—catch-all versus mass-party types—neither had any impact in a greater degree of participation in the online arena. What was found to determine the use of the political parties' websites was the size of the party, which we think is translatable to their budget. Thus, it is not politics but economics what weights in Spanish online politics.

This digital divide is contributing to political inequality in online terms (Gonzalez-Bailon 2008), as more resources allow for greater visibility, both in mainstream media as in the Internet.

So, late development of the Internet (compared to more advanced countries), trust in institutions and need for a critical mass or high budget seem to be the reason while online politics in Spain seem to still be, and in general terms, on a pre-Web 2.0 era. Findings by Borge et al. (2009) when analyzing local participation in Catalan municipalities can easily be extrapolated to the whole political Spanish landscape:

- In general, lack of infrastructure is a serious barrier for developing online strategies;
- When these strategies are at last developed, they are usually constrained to informative websites that have no place for deliberation tools;
- The population size seems again to be playing an important role in the presence of online politics at the local level, a conclusion that we feel quite related to budget rather than critical mass in terms of population;

[3] And the structure of Catalan politics is very similar to that of Spanish politics.

- Indeed, it is the abstention rate, the one that increases the probability of undertaking one or more participation initiatives;
- Unlike at higher government levels, left-wing mayors and independent candidatures tend to carry out more participatory processes, thus indicating that as the political machinery grows, usual rules (e.g., left-wingers are more participative) tend to apply less.

Some of the former points listed above—the role of abstention and the proximity of local politics being drivers of participation—provide us with a first idea on how the demand side of politics, the citizen, can look like.

A research carried on by Cantijoch (2009) showed that it is critical citizens who use the Internet more frequently for political issues, the reason being that they find in the online agora a place (still) not controlled by political, economical or media elites. This is not a contradiction with Jensen's findings (Jensen 2009),[4] but a complementary approach: citizens do not usually participate because they trust institutions, and it is the ones that do not, that are active on the Net. Adding to this, there is a pre-existing proclivity to use extra-representational modes of participation that is in fact reinforced by these people going online to bypass political elites.

On the other hand, she also saw that partisans and institution-believers would use the web more in 1.0 ways rather than 2.0 ways, or try and use 2.0 tools but with a central, coordinated, top-down approach, very far from the original nature of the Web 2.0. Extra-representational forms of participation have hence to be carefully analyzed as the purposes, goals, and final uses of them might differ, even if the tools used might be similar between institutionalized individuals and critical citizens.

Besides these two groups, a third one, the disaffected, would be using the Internet for many other purposes but politics. And the Internet would just not make a difference in their engagement.

The 'knowledge gap' (Tichenor et al. 1970) in the political system, where the more educated people would increase their information level on topics that were debated in relationship with their less educated peers, not only does not decrease, but it does increase due to a higher exposure to online information, becoming the Internet a gap increaser and not a knowledge leveler, as intuition might lead to think (Anduiza et al. 2009).

Notwithstanding, it is also possible that higher exposure to political information, found serendipitously on the Internet, can end up bringing the less interested in politics to higher levels of political knowledge.

To add up to the possible explanations of the low level of participation in Spain in politics online, we would like to go back again to the matters of e-readiness. Taking data from several sources, we recently showed (Peña-López 2008) that there is a strong relationship between e-readiness, political rights or political freedom, and participation. Though no relationships of causality or determinants were calculated, there were clear correlations between the level of development of the Information Society, education (which might also be related to the findings in

[4] In fact, both authors shared most of their datasets.

Anduiza et al. 2009), political rights or freedom, and how or at which intensity citizens would participate.

It would then be plausible to state that Spanish online politics are quite passive—quite 1.0-ish—part because of lag in digital development, part due to its inner political and institutional structure. On the other hand, when engaged online, activity is frantic and concentrated in educated, tech savvy and politically critical citizens.

In the following two sections we will analyze the two main activities by politicians and citizens in Spain, but in reverse order: firstly, the unripe state of political blogging; secondly the aspiration to lead online political campaigning.

8.5 Political Blogging

The ultimate sense of political blogging is to act as a counterweight to both the political power and the media power, many times the former determining the discourse of the later, and the rest of the times, the latter lobbying the former for their own interests.

If blogging has then to become a Fifth Estate (Dutton 2007), blogging has to be influent on the political agenda. Just after the first Internet-intensive US presidential campaign, the Institute for Politics, Democracy & the Internet (2004) identified and analyzed the political 'influentials' of that campaign and depicted their behavior online. Their main findings can be summarized as follows:

- Offline influentials are online influentials too; just rarely online influentials come out of the blue and pop up on the Internet;
- People—non influentials—look for them and value their opinions, which is what makes of them influential;
- Influentials are engaged people and are already very active within their communities;
- They are at the cutting edge of events, 2–5 years ahead the rest of the world in terms of what is going to come;
- They are deeply interested in politics and, if they do not pretend to make a change, at least they want to be aware of the changes;
- Poli-Influentials are people that are influential in many contexts and ways; they have usually (and significantly) reached a higher education level, with 60% of them being post-graduates;
- The more educated citizens are, the more influential activities people engage in, but in just the same proportion (online and offline, e.g., imparting a conference and writing an article) that other people not as much engaged;
- As expected, passive activities get the lion's share versus proactive activities in the ladder of engagement or activism.

The problem with the blogosphere is, nevertheless, the mere nature of the Internet, different from face-to-face relationships. If the IPDI already depicted a strong dependency of online engagement or influence from "real life" or offline

activities, Jacobson (1999) lists a wide range of reasons and variables why the same message could be understood in radically different ways, when communicated by online means.

Because of this, because of affinity and birds of a same feather flocking together more easily on the Net, because of a combination of both, there is a risk of people systematically flocking together to avoid misunderstandings and reinforce their own messages and points of view. Sunstein (2001) thus warns against the tendency that instead of being exposed to more and more plural information about politics, people will end up choosing only the information that represents their ideological views, creating a sort of 'daily me' and diffusing on and on the messages of the same kind. The addition of such individual behaviors in a friendly online community with end up creating echo chambers (Kelly et al. 2005; Kelly 2008) where just a few political messages will resonate: the ones with which we are comfortable and agree with.

Well, this is, more or less, what Criado and Martínez Fuentes (2009) seem to have found about the Spanish blogosphere during the Spanish local elections in 2007:

- The inexistence of the profile of a leader-blogger, as most bloggers have been emerged online without an offline authority, and offline influentials are not online;
- Parties still are the main broadcasters of information and communication, and have found no counter-power in the blogosphere;
- Indeed, when political blogging happens it is mainly personal, not mainstreamed, and depends a lot on the candidate's personality;
- Thus, blogs are but another campaign tool, not a 'blog' (in the sense of emergent participation of the Web 2.0) at all: they are unidirectional and highly mediatized.

This is most in line to what was found by Elmer et al. (2009) for Canadian politics and the Canadian blogosphere, which conclude that the political blogosphere is mainly made up of political acolytes that redistribute and echo the centralized messages of the party.

This is not to say that there is no dissent or that the online political landscape is monochromatic: actually, 'the structural affordances of the Internet are enabling political communication flows within and outside the liberal democratic institutions of interest aggregation' (Jensen 2009), but it definitely is not related with trust in institutions, partisan identification, and belief in political authorities. Disagreeing with Jensen, we then believe that the Web 2.0 might actually provide a counterpoint in form, but most probably not in content and hence unlikely to have an impact.

8.6 Campaigning

It is absolutely beyond any shade of doubt that campaigning has been reshaped because of the pervasiveness of the new digital media. In Howard's (2005) own words 'established political elites use database and Internet technologies to raise money, organize volunteers, gather intelligence on voters, and do opposition research.' In this sense, parties have increasingly entered and mastered—and even

conquered, many would say—online platforms to make their discourse and propaganda in both quantitative and qualitative ways: more available to more people, more focused and personalized for more specific profiles.

This is a 'more of the same' outcome of online politics, that is, reinforcing the voice of the ones that already had it: parties and political mainstream structures in general. Was the web 2.0 not said to be a participative, horizontal, plural platform and philosophy? If true, there are two possibilities for participation that could be happening. On the one hand, the possibility for politicians to have their own voice sent out of the party and the party's discipline (Hara 2008). On the other hand, the possibility for citizens to set up their own campaigns based on the possibility to individually broadcast and engage in a conversation (Castells 2007).

But the reality, at least in Spain, looks much more like the former—i.e., political institutions settling in the new virtual territories—than like the latter—individuals raising their own voice above the white noise of spin doctors' babbling.

According to Franco Álvarez and García Martul (2008), and based on their research of the Spanish presidential elections in 2008 and the role of citizen networks, the promise of a digital agora where plural voices can find a place and be heard is far from being true. Far from being a place for discussion and debate, the Internet is seen by political parties as yet another place where to harvest voters. Of course, being a new media, new(-ish) strategies are put to work so that their campaigns penetrate in each and every multimedia and online platform. But the result of it all, is that the digital sphere is conquered with yet the same message, making all media converge in the same, single message.

Indeed, what we find here is two types of athletes: the long distance runner, here represented by the apparatus of the party, and the speed racers and sprinters, which feature the activists and political critics. Amongst the latter, there might well be citizens that express out loud their political beliefs but without a real, deep, substantive engagement (Howard 2005), and the ones that engage in short run, cause-oriented forms of political participation (Norris and Curtice 2006) which fade out or shift towards other causes once the former has been achieved or its time has expired. And politics, if anything, is more of a marathon than a 100m race.

Thus, Jensen (2009) believes that 'political support and political participation are uncoupled: political support has little bearing on whether members of the political system participate.' In other words, the political system has not changed its own strategy, which is more related with winning elections than with promoting a deliberative democracy where building ideology and solutions is more important than staying in power.

Left with little room for participation, the politically engaged, use the Internet to get their information about politics but outside of the political apparatus, thus leaving aside the political party or governments as a conduit for political information, and instead looking for propaganda-less information and, presumably, more objective one. The problem with this behavior is that instead of leading towards a democratization of politics, it counter-intuitively feeds the informational divide or the knowledge gap (Anduiza et al. 2009) and unbinds political activism with political support. The promise of the universal agora becomes the nightmare

of a political Babel Tower, where debate is replaced by a bedlam where the powerful wants to keep, as always was, his voice heard over the herd.

In general, we see in Padró-Solanet (2009) that the online strategy of parties when campaigning—and that can be extended to their online presence in general—varies depending on them being on the government and the consequent electoral pressure, their political color and the ideological coherence, or the organizational weight. Notwithstanding, and in line with aspects we have already talked about, it looks like participatory tools are more used to create buzz against the government rather than build a (new) political project, and that the recognition and promotion of cyberactivism are more in the line of extending the party's tentacles rather than bringing in plurality and debate.

In their analysis of the Spanish presidential elections in 2008—arguably the first ones in Spain where the Internet played an important role—Peytibí et al. (2008) just reinforce what has been said so far: parties, partisans, and citizens got into online politics as if pushed by an invisible hand, but the overall result was unchanged politics—in form and in depth—and, in the worst cases, a static political scene where the promise of the Web 2.0 had burned out.

In this sense, all actors worked their hearts out on the Internet. Almost all tools at reach were used by parties, partisans and citizens: blogs, nanoblogs, 'crowdsourcing,' social networking sites, live video streaming, photo and video sharing sites, viral online strategies—and many of them fostered by parties themselves. The major change was the enablement of 'i-Campaigns,' where everyone connected had the capacity and opportunity to generate content for a party/candidate, without their intervention or even approval. Surprisingly, the i-campaigns often showed dissent with the party apparatus, especially when parties had or, recently had an internal crisis. This dissent, though, would only be channelled into better propositions when the dissident blogs had not a strong lobbying component or bloggers were not organized or near a political ideology. Again, the usual structure of inside-outside (of politics, of political parties) or the concurring monologues instead of the desired dialog.

8.7 Some Practical Examples to Pave Future Ways

If the landscape we have depicted so far is not very promising, there are several isolated—but increasingly intertwined—initiatives that make us feel optimistic and confident—or obstinate and stubborn about our own beliefs—about real Politics 2.0 gradually entering a territory now exclusively inhabited by the great mainstream parties (and their ideas) and the media corporations (and their interests).

We have picked up some experiences that we will very briefly describe below. There are many more, and the ones presented here have been chosen on a very personal and subjective way. Their inclusion here is to show some counterpoints to what has been stated so far in this chapter, leaving to the reader, the exercise to make abstraction of them, compared with the current mainstream situation, and

guess and wonder whether these are the first stages of a trend, or just sympathetic but early to fade initiatives.

8.7.1 The Power of Cyberactivism

On March 11, 2004, just 3 days before the presidential elections, Spain suffered the worst terrorist attack of its history. 191 people were killed and hundreds were hurt in bombings of commuter trains in the heart of Madrid, the Spanish capital.

Though the debate around the attacks is yet to be settled, there is common agreement that they were planned by an al-Qaeda terrorist cell and most probably as a revenge for the endorsement of the Spanish government to the invasion of Iraq in 2003.

Nevertheless, due to lack of data at that time or due to the pressure of the upcoming election, the Spanish government would report during the following days that it had been ETA, the Basque terrorist organization, the one behind the attacks. And it would keep reporting it despite the agreement of foreign media on the al-Qaeda hypothesis, foreign media that were accessed through the Internet by Spaniards and its information translated and diffused within the country and circumventing mainstream media.

In the days that followed March 11th, and until Election Day in March 14th, the discontent and loss of trust in the official (and presumably interested) version by the government led the citizens to mobilize in many ways (Traficantes de Sueños 2004), the most important one, the demonstration on March 13th, Reflection Day,[5] a grassroots demonstration summoned anonymously through a chain of mobile phone text messages that spread like gunpowder in hours.

Anonymous or triggered by the opposition to the government, the fact is that it reached huge momentum and caused invaluable damage to the government's public image. The demonstration, the terrorist attacks, or both, made the government lose the re-election, when previous days' polls took it for granted.

8.7.2 The Acknowledgment and Naturalization of Cyberactivism

The 37th National Congress of the Spanish Socialist Party (PSOE) in 2008 will be remembered by many because of the 'Facebook Amendment'.[6] Fostered by left-wing and sympathizers, and PSOE partisans and supporters, the 'amendment' wanted to amend the clause that gave the right to vote in party congresses,

[5] In Spain, it is absolutely forbidden to perform any kind of political act or declaration the previous day of Election Day.

[6] Some information about this process here: http://delicious.com/ictlogist/enmienda_facebook

committees and conferences through membership or delegation, and give this right to a broad base of cybermilitants. The amend was presented on many blogs and received important endorsement on the Facebook platform.

Though the amend did not pass, and most cyberactivists saw the decision as the old guard not understanding what the Internet was about, in many senses we believe it was just about the contrary.

On the one hand, it was explicitly acknowledging that the distinction between offline and online made no sense in politics (an in life in general), and that activism had to use all the tools at hand: there was just one activism, and different tools, and not many activisms depending on the tools.

On the other hand, the Facebook Amend made it clear that there was a big group of militants and members of the party that were concerned about Politics 2.0 and, more important, that had already engaged in their own crusade through blogs, nanoblogs, social networking sites. Thus, the debate around cyberactivism was formally open and structures to deal about the issue were committed within the party.

8.7.3 Blogging to Build and Weaved Blogging

'Las Ideas' (The Ideas) is a Spanish association created in March 2003 to promote culture, freedom, progress, constitutional values, human rights or equality. In fact, it is a left-wing think-tank that fosters political debate in an open and plural way,[7] being digital participation, e-democracy or e-government amongst the most dealt with topics.

Beside the content and level of reflection of Las Ideas—which might equally be the likes and dislikes of many—what cannot be denied is that they have brought the intersection of Information and Communication Technologies and Politics under the spotlight and in a non-scholar and, especially, non-arcane way. Indeed, they have been able to deploy online and offline tools to promote online politics and politics 2.0:

A website,[8] which actually is an aggregator of political blogs, featuring almost all of the most influent left-wing and political centre blogs; iCities, one of the more relevant conferences on Open Government, e-Administration and Digital Participation for non-scholars and non-professionals; and the 'Enrique Padrós' prize for the best political blog, with two categories: best professional politician blog, and best non-professional blog about politics.

Though an enormous echo chamber where ideas of the same color resonate on and on, Las Ideas certainly aims at bridging the spheres of professional politicians with supporters, and the offline sphere with the online one.

---

[7] Though increasingly less and less plural, in our very personal opinion, as they tend to close the circle of people and topics with which they relate with in their activities.

[8] See http://lasideas.es

8.7.4 Open Government, Open Parliaments

In early 2009, the Catalan Parliament issued their Parlament 2.0 project, on which they had been working the previous year. Boosted by the president of the parliament himself, Parliament 2.0 had two main branches. On the one hand, it would collect all the 2.0-ish initiatives of the members of the parliament.

First, along with their online profiles, the members of the parliament would see listed their digital profiles in whatever services 2.0 they wanted, including their own personal pages and blogs. Not only that, their updates (in the case of blogs and nanoblogs) would also be aggregated on a dedicated page within Parlament 2.0.

Second, the parliament would have its own presence on the most important Web 2.0 sites, and be using them according to their own particular norms of netiquette and usage. The parliament has accounts on YouTube, Facebook and Twitter, uses Netvibes to gather all its online activity and even provides widgets so that the society at large can follow the activities of the members of the parliament or the parliament as institution.

The acceptance of the initiative was terrific. Actually, some members of the parliament were already using Web 2.0 tools to prepare proposals or during sessions. Parlament 2.0 was an explicit endorsement to these behaviors, that have nevertheless been banned in other parliaments around Europe.

Just some months after Parlament 2.0 went public, the then new Basque Government (that took power in May 2009) appointed two renowned Spanish bloggers as director of the Office for the Modernization of the Administration and director of Citizen Service, respectively. These two bloggers, public servants of the Basque Administration, had won good reputation in matters of e-administration and e-government through their collaborative blog which they began in October 2005 and by taking part in debates on these topics at the national level.

These appointments were reinforced by the creation of the figure of the Chief Internet Officer of the Basque Government, whose main goal would be to initiate and build the Open Government during the new mandate.

Once more we found that acceptance, acknowledgement, and recognition of the digital debate on politics and politics (and administration and government) 2.0 was evident.

8.8 Conclusion

We have been seeing that there is an increasing will to engage online, from all sides of the political spectrum and for many reasons.

In general, politicians and parties see the Internet not as a new platform where new things can happen and old procedures can be reframed and reshaped: they see the Internet and ICTs in global as new communication media to be conquered. The party agenda to control the message, lack of digital tradition, lack of (real) participative tradition or lack of digital literacy are amongst the main reasons of this

philosophical approach. Of course, the Spanish political system does not incentivize going online for fundraising reasons—quite a powerful reason—so only creating a discourse and engagement remain as the main driver to go online, and they do not seem to be a priority beyond controlling this discourse and appropriating dissent.

We have also seen that there are not many differences amongst the behavior of the different parties, online or offline media and communication practices. Differences, as in 'real life' come more with capability (budget) rather than ideology, or come from specific persons acting as individuals rather than party or collective strategies.

We are nevertheless witnessing how shy, new initiatives struggle to break the status quo, most of the times against the political apparatus and mainstream media. The wish of renewal is still in the hands of tech savvy partisans and 'goverati'[9] that have yet to succeed in gathering a critical mass of followers, in gaining momentum, in performing a non-disruptive transition that scares, not convinced but still reluctant politicians, and citizens. Indeed, these tech savvy individuals have also to fight the fact of low levels of Internet intensive usage, which is especially in higher age segments, which are the ones that do rule the country.

We would like to end this chapter with some lessons learned and some recommendations. Though grounded in literature and direct experience, these are personal opinions and, as such, should be taken with a grain of salt:

First, the debate about offline versus online is, we believe, artificial and counterproductive. The mere idea that there might be 'web users' versus 'normal/real people' seems to us outrageous, as there is nothing behind 'web users' but 'real people.' That said, if there is to be a change in online politics it can only come through a change in 'real' politics. We have already mentioned the Spanish political system and how it is funded. We could add to that how candidates are elected (primaries, open vs. closed lists) or how party-centered (vs. candidate-centered) are politics in Spain, with its biases towards party discipline (in all senses, including thinking and having an opinion or one's own) in detriment of genuine debate. Changes in this sense will find in the Web 2.0 and Politics 2.0, perfect tools to leverage new strategies. But these tools, without the prior changes, is like having hammers to unscrew nuts.

Second, e-readiness and digital literacy and competences are, definitively, a major barrier. Simply enough, online politics require digital access. But beyond physical access, complex digital competences are a must for serious online engagement, especially when the pace of technological change is so quick and stressing. We should by all means learn to read statistics on the Information Society, and tell Internet users from people that are able to use the Internet to achieve their own personal and professional goals, which take the most benefit from digital tools.

[9] For a brief explanation of the concept goverati please see Drapeau 2009. For a longer reflection about the topic, Peña-López 2009a; Peña-López 2010.

Third, the former two points can be added up in this third one: online politics and Politics 2.0 is not about a revolution, but about an evolution. Disruptions cause uneasiness in people and hence resistance, resistance to change. Evolutions are often seen as improvements of actual situations, while revolutions have historically had collateral damages and direct casualties, which is always frightening. Only by agreement and guidance, can the benefits of the evolution be clear. Which leads us to the last point.

Fourth, the Web 2.0 offers us a change towards Politics 2.0. Change is usually an investment, which is almost surely a cost. The cost of Politics 2.0 is, above all, that, somehow, we go our way back from representative democracy to a more direct or deliberative democracy. Criticized as it is for its inefficiencies, inefficacies, corruption and personal interests biases, representative democracy is though a comfortable, cozy, cheap (in terms of personal time and resources), even lazy framework where to be a citizen. Engagement consumes energy, personal energy, and we have yet to find the Energy 2.0 to feed it.

References

Anduiza E, Gallego A, Jorba L (2009) The political knowledge gap in the new media environment: evidence from Spain. Prepared for the seminar citizen politics: are the new media reshaping political engagement? Barcelona, 28–30 May 2009. IGOP, Barcelona

Arnstein SR (1969) A ladder of citizen participation. J Am Inst Plann 35(4):216–224. American Institute of Planners. http://lithgow-schmidt.dk/sherry-arnstein/ladder-of-citizen-participation.pdf

Batlle A et al (2007) Reconsidering the analysis of the uses of ICTs by political parties: an application to the Catalan case. Communication presented at the 4th ECPR General Conference. Pisa, ECPR. http://www.essex.ac.uk/ecpr/events/generalconference/pisa/papers/PP669.pdf

Bimber B, Davis R (2003) Campaigning online. the Internet in U.S. elections. Oxford University Press, Oxford

Borge R (2005) La participación electrónica: estado de la cuestión y aproximación a su clasificación. Revista de Internet, Derecho y Ciencia Política 1. Barcelona, UOC. http://www.uoc.edu/idp/1/dt/esp/borge.pdf

Borge R, Colombo C, Welp Y (2009) Online and offline participation at the local level. A quantitative analysis of the Catalan municipalities. Information, Commun Soc 12(6):1–30

Cantijoch M (2009) Reinforcement and mobilization: the influence of the Internet on different types of political participation. Prepared for the seminar citizen politics: are the new media reshaping political engagement? Barcelona, 28–30 May 2009. IGOP, Barcelona

Castells M (2007) Communication, power and counter-power in the network society. Int J Commun 1:238–266. USC Annenberg Press, Los Angeles. http://ijoc.org/ojs/index.php/ijoc/article/view/46/35

Chadwick A (2009) Web 2.0: new challenges for the study of E-democracy in an era of informational exuberance. J Law Policy Inform Soc 5(1):9–41. State University, Columbus. http://www.is-journal.org/V05I01/Chadwick.pdf

Chadwick A, Howard PN (2008) Routledge handbook of Internet politics. Routledge, New York

Cornfield M (2005) The Internet and campaign 2004: a look back at the campaigners. Washington DC, Pew Internet & American Life Project. http://www.pewinternet.org/pdfs/Cornfield_commentary.pdf

Criado JI, Martínez Fuentes G (2009) ¿Hacia la conquista política de la blogosfera? Blogging electoral en la campaña de los comicios municipales del 2007. Revista de Internet, Derecho y Ciencia Política 8. Barcelona, Universitat Oberta de Catalunya. http://idp.uoc.edu/ojs/index.php/idp/article/viewFile/n8_criado_martinez/n8_criado_esp

Cristancho C, Salcedo J (2009) Assessing Internet mobilization—integrating Web analysis and survey data. Prepared for the seminar citizen politics: are the new media reshaping political engagement? Barcelona, 28–30 May 2009. Barcelona, IGOP

Davies T, Peña Gangadharan S (eds) (2009) Online deliberation. Design, research, and practice. CSLI Publications, Stanford. http://odbook.stanford.edu/static/filedocument/2009/11/10/ODBook.Full.11.3.09.pdf

Drapeau M (2009) Government 2.0: The rise of the Goverati. In: ReadWriteWeb, 5 February 2009. http://www.readwriteweb.com/archives/government_20_rise_of_the_goverati.php

Dutta S, Mia I (eds) (2009) Global information technology report 2008–2009: mobility in a networked world. Palgrave Macmillan, Basingstoke. http://www.weforum.org/pdf/gitr/2009/gitr09fullreport.pdf

Dutton WH (2007) Through the network (of networks)—the Fifth Estate. Inaugural lecture, Examination Schools, University of Oxford, 15 October 2007. Oxford Internet Institute, Oxford. http://people.oii.ox.ac.uk/dutton/wp-content/uploads/2007/10/5th-estate-lecture-text.pdf

Elmer G et al (2009) 'Blogs I Read': Partisanship and party loyalty in the Canadian political blogosphere. J Inform Technol Polit 6(2):156–165.

Fleishman-Hillard (2009) European parliament digital trends. Fleishman-Hillard, Brussels. http://www.epdigitaltrends.eu/uploads/downloads/FH-Digital_Trends_report.pdf

Franco Álvarez G, García Martul D (2008) Los efectos de las redes ciudadanas en la campaña electoral del 9-M. Ámbitos 17:25–36. Universidad de Sevilla, Sevilla. http://grupo.us.es/grehcco/ambitos17/02Franco.pdf

Gibson RK (2009) New media and the revitalisation of politics. Representation 45(3):289–299.

Gonzalez-Bailon S (2008) The inner digital divide: How the web contributes (or not) to political equality. Working paper number 2008-02. University of Oxford, Oxford. http://www.sociology.ox.ac.uk/research/workingpapers/2008-02.pdf

Hara N (2008) Internet use for political mobilization: Voices of the participants. First Monday, 7 July 2008, 13(7). http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2123/1976

Hillygus S, Shields T (2007) The persuadable voter: campaign strategy, wedge issues, and the fragmentation of American politics. Princeton University Press, Princeton

Howard PN (2005) Deep democracy, thin citizenship: the impact of digital media in political campaign strategy. Ann Am Acad Pol Soc Sci 597(1):153–170.

Institute for Politics, Democracy & the Internet (2004) Political influentials online in the 2004 Presidential campaign. The George Washington University, Washington DC. http://www.ipdi.org/UploadedFiles/political%20influentials.pdf

Jacobson D (1999) Impression formation in cyberspace. J Comput Mediat Commun 5(1). doi: 10.1111/j.1083-6101.1999.tb00333.x

Jensen MJ (2009) Political participation, alienation, and the Internet in the United States and Spain. Prepared for the seminar citizen politics: are the new media reshaping political engagement? Barcelona, 28–30 May 2009. IGOP, Barcelona

Katz JE, Rice RE, Aspden P (2001) The Internet, 1995–2000: access, civic involvement, and social interaction. American Behaviorial Scientist 45(3):405–419.

Kelly J (2008) Pride of place: mainstream media and the networked public sphere. Media Re: public side papers. Berkman Center for Internet and Society at Harvard University, Cambridge. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/PrideofPlace_MR.pdf

Kelly J, Fisher D, Smith M (2005) Debate, division, and diversity: political discourse networks in USENET Newsgroups. Paper prepared for the Online Deliberation Conference 2005. Stanford University, Palo Alto. http://www.coi.columbia.edu/pdf/kelly_fisher_smith_ddd.pdf

Kirkman G et al (eds) (2002) Global information technology report 2001–2002: readiness for the networked world. Oxford University Press, New York

Morozov E (2009) How dictators watch us on the web. Prospect, December 2009, 165. Prospect Publishing Limited, London. http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/

Norris P, Curtice J (2006) If you build a political Web site, will they come? The Internet and political activism in Britain. Int J Electron Gov Res 2(2):1–21.

Noveck BS (2005) A democracy of groups. First Monday 10(11). http://firstmonday.org/issues/issue10_11/noveck/index.html

Noveck BS (2008) Wiki-government. Democracy (7):31–43. http://democracyjournal.org/article.php?ID=6570

O'Reilly T (2005) What is Web 2.0. O'Reilly, Sebastopol. http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

Oates S, Owen D, Gibson RK (eds) (2006) The Internet and politics. Citizens, voters and activists. Routledge, New York

Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (2009) Evolución de los usos de Internet en España 2009. ONTSI, Madrid. http://observatorio.red.es/hogares-ciudadanos/articles/id/3650/evolucion-los-usos-internet-espana-2009.html

Padró-Solanet A (2009) The strategic adaptation of party organizations to the new information and communication technologies: a study of Catalan and Spanish parties. Paper prepared for presentation at the Workshop 20: parliaments, parties and politicians in cyberspace, ECPR Joint Sessions Lisbon, 14–19 April 2009. ECPR, Lisbon. http://intradociep.upmf-grenoble.fr/Spip//IMG/pdf/ECPR2009Padro-Solanet.pdf

Peña-López I (2008) Ciudadanos Digitales vs. Insituciones Analógicas. Conference imparted in Candelaria, 9 May 2008 at the iCities Conference about blogs, e-Government and digital participation. ICTlogy, Candelaria. http://ictlogy.net/presentations/20080509_ismael_pena-lopez_ciudadanos_digitales_instituciones_analogicas.pdf

Peña-López I (2009a) Goverati: new competencies for politics, government and participation. Seminar at the course: digital competences: knowledge, skills and attitudes for the network society. CUIMPB, 16 July 2009. ICTlogy, Barcelona

Peña-López I (2009b) Measuring digital development for policy-making: models, stages, characteristics and causes. Ph.D. thesis (mimeo)

Peña-López I (2010) Goverati: e-Aristocrats or the delusion of e-Democracy. In: Parycek P, Prosser A (eds) EDem2010. In: Proceedings of the 4th international conference on e-democracy, 23-39. Österreichische Computer Gesellschaft, Wien. http://ictlogy.net/articles/20100506_ismael_pena-lopez_-_goverati_e-aristocrats_delusion_e-democracy.pdf

Pew Research Center for the People & the Press (2008) Social networking and online videos take off. Internet's broader role in campaign 2008. Pew Research Center for the People & the Press, Washington DC. http://people-press.org/reports/display.php3?ReportID=384_

Peytibí FX, Rodríguez JA, Gutiérrez-Rubí A (2008) La experiencia de las elecciones generales del 2008. Revista de Internet, Derecho y Ciencia Política 7. Barcelona, Universitat Oberta de Catalunya. http://www.uoc.edu/idp/7/dt/esp/peytibi_rodriguez_gutierrez.pdf

Robles JM (2008) Ciudadanía Digital. Un acercamiento a las causas de la ideología de los internautas españoles. Research seminar held on 3 July 2008 in Barcelona, Universitat Oberta de Catalunya, mimeo

Smith A (2008) Post-election voter engagement. Pew Internet & American Life Project, Washington DC. http://www.pewinternet.org/pdfs/PIP_Voter_Engagement_2008.pdf

Smith A, Rainie L (2008) The Internet and the 2008 election. Pew Internet & American Life Project, Washington DC. http://www.pewinternet.org/pdfs/PIP_2008_election.pdf

Sunstein CR (2001) Republic.com. Princeton University Press, Princeton

Tichenor PJ, Donohue GA, Olien CN (1970) Mass media flow and differential growth in knowledge. Public Opin q 34(2):159–170.

Traficantes de Sueños (ed) (2004) ¡Pásalo! Relatos y análisis sobre el 11-M y los días que le siguieron. Traficantes de Sueños, Madrid

Part III
Policy Dimensions: Surveillance

Chapter 9
The Normality of Living in Surveillance Societies

David Murakami Wood and C. William R. Webster

Abbreviations

CCTV Closed Circuit Television
ICT Information and Communication Technology

Contents

9.1 Introduction 152
9.2 Global Surveillance and the Domestication of Security 153
9.3 Normalizing Surveillance Society 155
9.4 Everyday Life in Surveillance Societies 157
9.4.1 Aspect 1: Contrasting Perceptions of Surveillance 158
9.4.2 Aspect 2: Depth of Surveillance 159
9.4.3 Aspect 3: Exposure to Surveillance 159
9.4.4 The Emergence of Surveillance Societies 160
9.5 Concluding Discussion 161
References 162

Contribution received in 2010.

D. M. Wood
Department of Sociology, Queens University, Kingston ON, Canada
e-mail: dmw@queensu.ca

C. W. R. Webster (✉)
University of Stirling, Stirling, UK
e-mail: c.w.r.webster@stir.ac.uk

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_9,

9.1 Introduction

It is increasingly argued that contemporary capitalist nations have become 'surveillance societies' in which surveillance related activities are embedded as the core mode of organization, production and societal order (Lyon 1994, 2001, 2007). But what does it mean to live in a surveillance society and what economic, political and social relations are produced? These are the key questions addressed in this chapter.[1] In particular, the chapter argues that technologically mediated surveillance is becoming normalized across Europe and that this is altering the landscape of liberty, security and citizen-state relations. It identifies this normalization as a product of the globalization of surveillance, the domestication of security, and the influence of surveillance pioneers, such as the United Kingdom. The underlying theme of the chapter is that we should abandon the notion that we are still 'discovering' surveillance and that we should instead see surveillance as a normal part of everyday life (Murakami Wood and Webster 2009). Moreover, the normalization of surveillance in social life has important ethical and political consequences, which although inevitable for everyday life, should be examined in more detail. In this respect, the chapter argues that it is important to not only account for the ways in which surveillance occurs, but to critically examine the increasingly coherent and stable surveillant assemblage (Haggerty and Ericson 2000). Supporting this argument is the simple proposition that technologically mediated surveillance practices raise significant questions about modern society, the nature of liberty and privacy and their relationship to security, and about relations between citizens, businesses and the state. Furthermore, a closer examination of the 'new normality' of everyday surveillance highlights the differentiated and diverse application of surveillance across different nations.

The chapter is organized around three main sections. The first section sets out the ways in which surveillance has become a key part of the 'organizational package' embedded in modern capitalism. Here it is argued, that contemporary globalization involves the simultaneous spread and intensification of this particular mode of capitalism, but also forms of governmentality, state, social and personal organization that accompany it, flow 'naturally' from the adoption of these new relations of production and consumption. The second section considers the normalization of surveillance in society by exploring the provision of video surveillance or CCTV (Closed Circuit Television) cameras and systems in the UK. In particular, this section explores the ways in which surveillance has been embedded into the general fabric of modern life. The third section explores the nature of modern surveillance for those living in surveillance societies. This is achieved by exploring dimensions of modern technologically mediated surveillance, dimensions which show that surveillance is subtle, deep, unobtrusive and selective. By highlighting the degree to which surveillance is embedded in modern society we

[1] These are also the key questions being addressed by the Living in Surveillance Societies (LiSS) COST Action ISO807 (2009-13), <www.liss-cost.eu>. Contribution received in 2010.

hope to stress the importance of seeing surveillance as an important policy issue and to make policy-makers and practitioners more aware of the surveillance polity around us.

9.2 Global Surveillance and the Domestication of Security

The emergence of surveillance as a key feature of modern society is clearly intertwined with military activity, the domestication of security and the development of a global surveillance industry. It is often argued that modes of production and consumption have their own accompanying modes of ordering (see for example; Law 1992) and in recent years that surveillance has become the key mode of ordering in modern capitalism (Lyon 1994, 2001, 2007). This has been the result of certain socio-technical developments, and in particular, developments in telecommunications and computing which have been utilized to realize new products and services. New technologies support the new mode by collecting and sorting data on people, things and events, in order to produce categories of risk and profitability, which will enable foresight and the anticipation of future risks and profits. Although many of these developments have initially taken place in military arenas the globalization of surveillance is accompanied by the domestication of security as surveillance practices and behaviors transfer from military to normal life. As the 'risk-surveillance society' (Coaffee et al. 2009) has become the 'ideal-type' state of the 21st century, so its aims—anticipated and pre-managed risk, safety, control, security—are increasingly permeating policy and practice at every level. The relationship between globalization and militarism has not gone unnoticed and a number of authors have commented on the militaristic nature of contemporary capitalism and the significance of the military for the growing security industry and the growing desire for a 'secure' society (see for example; Coaffee et al. 2009; Hardt and Negri 2000; Klein 2008).

The global surveillance economy has its roots in the post-Cold War period. In this era there was a diversification of production in the military security sector whereby large companies that had previously been military contractors adapted their products and services for civilian markets (Coaffee et al. 2009). For example, the Automatic Number Plate Recognition system installed in London in the early 1990s relied on technologies tested during the invasion of Iraq in 1991. This transfer of military terminology, practices and technologies, from the military arena to domestic public policy and services, has been led by a number of US and European companies and has resulted in the emergence of a large and lucrative surveillance economy. The new surveillance economy has profited from the renewed hostilities that have gradually come to fill the perceived military vacuum left by the collapse of the Soviet Union. Along with the creation of new civilian markets for military surveillance equipment, the language of combat has also become part of the lexicon of politics and public policy: the 'war on drugs,' the 'war on crime,' and as Ericson (2006) puts it, a 'war on everything.' The 'war' on

terror(ism) and the invasions of Iraq and Afghanistan signal a marked development in the use of surveillance technologies and a significant surge of military techno-surveillance development. The new 'war' does not involve the massive, lumbering, traditional 'baroque arsenal' (Kaldor 1981) but is a series of asymmetric conflicts seen as being fought much more through information and intelligence than through the threat of total violence and annihilation (Metz 2000; Graham 2004). In a similar vein, policing has evolved and is now information-led and targeted. The new forms of war and crime are also international, transnational and intranational, they do not match the old national order, and therefore can be seen to call into question the capacity of both existing global institutions, such as the United Nations or Interpol, and individual nation-states to deal with these issues (Loader and Walker 2007).

The new forms of international security cooperation and the setting of surveillance standards are embedded in a new surveillance economy being shaped and led by the US (Hardt and Negri 2000) and Europe. Much of this activity is secretive and there is a dense network of cooperating agencies and practices. The extent and nature of this network is highlighted by the CHALLENGE programme[2] which demonstrates the degree to which European political elites closely allied to the security industry are taking a leadership role in the development and deployment of surveillance practices and systems. Although, there seems to be a degree of trans-Atlantic cooperation Europe is quite capable of developing its own systems and practices, as demonstrated by the Galileo satellite project, which will create a direct rival for the US Global Positioning System (Lembke 2002; MacDonald 2007). The European Union has also created its own 'Fortress Europe' Schengen immigration controls (Bigo and Guild 2005) and has frequently gone beyond the standards required by international agreements on surveillance and security. The latter point can be demonstrated by the development of the new EU biometric passport (Bunyan 2005).[3]

The emergence of new modes of surveillant organization and the expansion of military technologies into civilian markets has led to a redefinition of the concept of security. Security is no longer a national issue—national security—it is also, at the same time, an international issue and a domestic or civil issue. For example, it is clearly the case that many forms of surveillance, especially those associated with crime control and policing, can be seen as a domestication of military security rationality alongside the use, in many cases, of military technologies—what Murakami Wood refers to as 'security coming home' (Murakami Wood et al. 2006). The domestication of surveillance technology occurs not just in the arena of urban security and surveillance but also in practices of government. There has been a migration of technologies from military settings to civil settings driven by the expansion of e-government services and the need for more effective and

[2] CHALLENGE, EU framework program 6-funded research network on liberty and security: <http://www.libertysecurity.org/>.

[3] See also Chaps. 13, 14 and 23 of this book.

efficient public services. The use of new ICTs has led to the emergence of large state databases, designed for processing public service information, and the emergence of new transactional electronic public services, using a range of electronic service delivery mechanisms, including the Internet (Bellamy and Taylor 1998). These developments utilize the networked computing infrastructure which was initially a product of US Cold War military research and development and an attempt to create a 'closed world' over which the US military could exercise control (Edwards 1996).

9.3 Normalizing Surveillance Society

The domestication of security and the globalization of surveillance would be limited processes if their activities did not become an increasingly 'normal' part of everyday life. In his critique of Foucault, Agamben (2005) describes the way 'states of exception' spread and come to be expected forms of governmentality. What in the previous mode of ordering would be regarded as temporary or even entirely unacceptable becomes unremarkable, mundane, and normal. A good example is the diffusion of video surveillance or CCTV cameras and systems, especially in the UK (Webster 1996, 2004). Beyond early experiments (Williams 2003, 2009), the history of state video surveillance in the UK began in the late 1980s and went through a period of massive expansion during the mid-1990s and again in the early part of the twentieth century (Webster 2009). What is remarkable about this diffusion is not just the speed of the spread of cameras and systems but the lack of opposition to their introduction, the general enthusiasm for their deployment and the demand to install them in more and more places. This is all the more remarkable given that detailed evaluations of systems have repeatedly suggested that CCTV is extremely limited in its effectiveness in preventing and deterring crime (see for example Welsh and Farrington 2002; Gill and Spiggs 2002). CCTV has therefore been criticized as an extremely inefficient use of public funds (Groombridge 2008) and for its impacts on liberty and social trust (Murakami Wood et al. 2006).

This of course leads us to ask why we have installed so many CCTV cameras and systems and why is there no effective opposition to their introduction? There are several potential explanations. Firstly, it could be about what they represent rather than what they do, and in this perspective it doesn't really matter what they do. CCTV cameras are a visible manifestation of the state's concern about crime and security, they demonstrate 'something is being done' in the 'fight against crime.' This is immensely important to politicians who have to justify their existence and actions. In this respect, CCTV is 'stage-set security' (Coaffee and Murakami Wood 2006) or 'security theatre' (Schneier 2008) and gives us a symbol of safety in a society in which everything is seen as a potential source of risk and where fear dominates. Theatrical security can be found everywhere from the airport to the high street, from the demand to remove shoes for inspection to the

increasing numbers of uniformed 'plastic police' (Police Community Support Officers, Neighborhood Wardens, private security guards and the like), who look like the 'real' police but lack their training and powers. These are all symbols of order in the 'security theatre.'

Secondly, CCTV is being installed for a variety of purposes and may be much more effective in areas other than the fight against crime. For example, CCTV has proved extremely useful in directing police resources, gathering intelligence and alleviating the fear of crime. Furthermore, their introduction should not solely be interpreted as a 'nasty' surveillance activity but also a paternalistic state activity whereby the state is trying to 'look after us.' Lyon (2001) argues that the motivations for surveillance are usually as much about care as they are about control and if CCTV cameras imply the notion of someone watching, for many people this means watching out for them. However, in practice those working in CCTV control rooms have limited training and have to undertake hours (upon hours) of monotonous surveillance. There may be examples of care, but there are also examples of bad practice, including surveillance for personal titillation via the compilation of sexual images of women from recordings by male operatives (Norris and Armstrong 1999; Smith 2004, 2007).

Thirdly, CCTV has quickly become part of the cultural landscape of the UK (Groombridge 2002) with CCTV images being utilized for mainstream entertainment. In this respect, the media has driven the normality of surveillance and the normality of participating in a surveillance society. Typically, programs using CCTV footage stress the effectiveness of the police in chasing and catching criminals and reinforced the growth of reality based TV programs. A second wave of reality TV developed where the 'reality' was created for the purposes of entertainment, for example a group of young people in an expensive studio apartment or on a deserted island—but constantly surveyed via surveillance cameras and broadcast 24/7. Much like the operators in a CCTV control room, the millions of viewers in this 'synopticon' (Matthiessen 1997) watched these small groups of voluntarily incarcerated individuals in the generally frustrated expectation that something might happen. It was banal, boring, normal, and utterly addictive. However, there is a more productive governmental aspect to the watching of surveillance images. Andrejevic (2003) and Palmer (2003) have drawn attention to aspects of socialization attached to this kind of watching. For them, it is a process of governance (Palmer) and a kind of labor (Andrejevic), a form of training for both participants and watchers. In effect this helps us all to become used to surveillance, to experience it as an expected part of everyday life, to enjoy it and to watch its products in a certain way, and to train our eyes and minds for surveillance. In this way, we all become 'agents of surveillance' as we personally take on the responsibility to 'look out for suspicious activity' (Coaffee et al. 2009), what Rose refers to as the 'responsibilization' of citizens (2000).

A significant aspect of this discussion is that none of these arguments have anything to do with the technical properties of the CCTV cameras and systems or the actual functioning of the systems per se. They are not about precisely accounting for the numbers of cameras, their capabilities, or about whether the

cameras 'work' or not. Instead, our argument is about how surveillance works at the emotional level, the way it is embedded in everyday culture and is symbolic of modern society. The normalization of surveillance occurs when surveillance colonizes these domains. The normalization of surveillance is therefore also about far more than just the proliferation of a range of surveillance artifacts and technologies—it is about how these are embedded in the institutions and norms of society and how they are reflective of other aspects of modern society.

There are other aspects of this 'normalization' process which are as equally significant, and in particular, alterations to routine work practices and management procedures around new ICTs in government and public service settings. The move to computerized, information intensive, networked, electronic public services has been driven by cost cutting and efficiency agendas, partly because new informated services are replacing paper-based manual services and partly because new electronic services allow citizens to access services from multiple locations at their own convenience. The electronic provision of public and democratic services also leads to the emergence of large state databases and the possibility of information sharing (Varney 2006). Furthermore, these technologies allow for the emergence of citizen-centric or citizen-focussed services, where new technologies tailor information specifically for individual citizen clients (Taylor et al. 2009). Services are therefore personalized around the discreet information and needs of individuals, surveillance is seen to be working to provide what citizens want, and without it, these services would be put at risk. Again, this reinforces the normality of the collection, storage and sorting of large amounts of personal data, and the 'ownership' of personal data by the state. The emergence and evolution of electronic public services are key to developing a surveillance infrastructure, to populating it with information, and importantly, because of the universal and information-intensive nature of public services, bureaucrats, citizens and service users are all exposed to subtle surveillance practices through the everyday interactions that occur around information giving/sharing and service provision. Interactions become structured around surveillance relationships and the new forms of social negotiation that emerge are no longer about what information one chooses to give but how that information is to be given (or taken).

9.4 Everyday Life in Surveillance Societies

Global surveillance and the domestication and normalization of surveillance has led a number of authors to explicitly consider 'life' and everyday living in the emerging surveillance society (Aas et al. 2008; Lyon 2001; Monahan 2006). The term 'surveillance society' is widely recognized and in recent years has gained considerable currency. It is also a bland term, although it recognizes the widespread use of surveillance technologies in society it tells us little about how these technologies are felt, experienced or the different dimensions and deviations in surveillance practice. Surveillance in the most basic surveillance society perspective is seen to

be ubiquitous and universal—everywhere—and mediated by new sophisticated ICTs. Such a position masks the subtleties of modern surveillance and the different ways in which we experience everyday life under the scrutiny of surveillance. This line of argument is explored further through the identification and exploration of three aspects of everyday surveillance, aspects which reflect upon: our perceptions of surveillance, the 'depth' of surveillance and our exposure to surveillance. The term surveillance society is further problematized by considering the different national settings for surveillance activity.

9.4.1 Aspect 1: Contrasting Perceptions of Surveillance

The first aspect relates to the different ways in which surveillance technologies are perceived, both in their desirability and their usefulness. The term 'surveillance society' has embedded in it a sense of negativity. It is a subjective term and conjures up images of a big brother state, the mass control of citizens and threats to privacy and liberty (Garfinkel 2000). This is reflected in popular literature, for example George Orwell's '1984' (1949), and in official reports, such as, the European Parliament Scientific and Technological Options Assessment Committee Report on 'Technologies of Political Control' (STOA 1998) or the UK's Information Commissioners Office report on the surveillance society (Murakami Wood et al. 2006). The deployment of surveillance technologies divides opinion and for many their introduction is heralded as valuable in delivering national security and in the 'fight against crime' and terrorism. This is demonstrated, for example, by the widespread support for CCTV in public perception surveys (see, for example, Honess and Charman 1992). Further to this, vast quantities of personal information are collected, stored and exchanged by public services in e-government initiatives designed to make public services more efficient, accessible and effective. In this respect, technologies, like CCTV, identity cards, offender tags, mobile phones, databases, the internet and sat nav, represent technologies for enhanced surveillance on the one hand and technologies of efficiency, enhanced services and a better, safer society on the other. Taylor et al. (2009) go so far as to argue that these two positions, that is 'information capture' for enhanced services and 'information capture' for surveillance, are diametrically opposed perspectives of the same phenomena—they call these two perspectives the 'surveillance state' and 'service state' perspectives. This dichotomy raises questions about the intentions of technological uptake and about our perceptions of these intentions. Following on from the argument brought forward by Taylor et al. (2009) the integration and networking of government databases could be seen as either effective 'joined-up' government or 'surveillance creep,' depending upon which perspective you subscribe to. Although these perspectives may seem diametrically opposed we would argue that they are not mutually exclusive and that it is actually possible to deliver public service efficiencies, enhanced security and increased surveillance simultaneously—this is what is happening in practice. The adoption of sophisticated new

technologies does not imply a choice between the surveillance society and a safe efficient society, because they are both happening simultaneously.

9.4.2 Aspect 2: Depth of Surveillance

The second aspect relates to the direction and intensity of modern surveillance. In the surveillance society perspective surveillance is seen as ubiquitous, it is everywhere and we are all subject to it on an ever increasing scale. However, we would argue that to suggest surveillance is everywhere masks the extent and depth of surveillance that can be realized through new technology. Furthermore, surveillance is more discreet than this. More often than not we are not aware that surveillance is taking place and consequently of the scope or scale of surveillance we participate in. Consider, for example, the spread of biometric ID cards or CCTV systems with facial recognition, both offer systems for electronic citizen identification, which can be networked to further databases to access a range of information about the citizen, potentially including information about their criminal, health, educational financial and/or employment histories. Such information could be extended beyond public records to include intimate information relating to personal relations, political affiliations, travel history and sexual preferences, etc. The point we are trying to make, is not what information is accessed, but our awareness of information sharing practices supported by discreet electronic interactions. We would argue, that most people are not aware of the information held about them, or what information is shared between agencies, and when. This scenario is only possible with the existence of large databases of personal information—and these databases exist in the public and private sectors. In addition to the records held by public service agencies the private sector keeps records about our credit history, our travel patterns (via sat nav and mobile phones), telephone and email usage and our purchase patterns (via loyalty cards like Nectar or the Tesco Clubcard). This information can be used to 'profile' individuals so that products can be selected and tailored to their personal requirements. Consequently, participation in modern society necessitates a series of activities which leave a data trail as we go about our everyday existence (Lace 2005) and many of these electronic interactions go unnoticed and are/seem perfectly normal. In this respect surveillance is not just ubiquitous it is deep, unobtrusive and sophisticated.

9.4.3 Aspect 3: Exposure to Surveillance

The third aspect relates to the extent to which we as individuals are the discreet targets of surveillance activity, that is, the extent to which we are exposed to intense technologically mediated surveillance. Although the surveillance society perspective would suggest we are all exposed to increasing levels of surveillance,

much of our exposure is benign and unobtrusive. This is because the majority of our electronic interactions, when considered on their own, are relatively insignificant (beyond the initial transaction or purpose of the interaction) and consequently do not warrant further surveillance attention. For example, travel cards, such as the 'Oyster' card in London, may record our personal travel details but they also provide important information about general travel patterns, such as passenger numbers on a particular route, peak periods, typical journey length, and so on. For the latter our personal details are not of interest, the value of the information gained relates to a bigger picture, what is of interest here is how this information can be 'reflected back' and utilized to make adjustments to service provision in order to provide better, more efficient services. In this scenario citizens and service users remain relatively anonymous, although they are surveyed, their personal details are not utilized in a meaningful way. This may be the case for the majority, but there will be instances where the same systems will be utilized to conduct intensive targeted personally focused surveillance. A case in point is the general use of CCTV in public spaces. Although such systems are commonplace (Webster 1996, 2004) their deployment has led to diverse surveillance practices and differentiated levels of surveillance (Webster 2009). Most citizens will pass through CCTV surveyed areas relatively anonymously, unidentified and ignored. However, certain individuals will attract further attention, scrutiny and surveillance. They may be exhibiting suspicious behavior, be known to the CCTV operatives, or just seem somehow different (Smith 2007). Such individuals may be surveyed more closely, their movements and activities more closely monitored. They are not anonymous, rather they are being subject to targeted intense surveillance. The key feature of this aspect is that our exposure to surveillance is differentiated by who we are or who we are perceived to be. Surveillance for one person may be unobtrusive, but for others it will be intense and pervasive. A further dimension of this argument relates to the vast quantities of personal data held. Individuals may not be 'live' surveillance targets but the trail of electronic information stored on databases mean that activities can be recalled at a later date if necessary. Given the right (or wrong) circumstances we can all retrospectively become surveillance targets—which of course means we are actually always already potential suspects.

9.4.4 The Emergence of Surveillance Societies

Despite the growing 'popularity' of the term 'surveillance society' its use masks an important dimension in the development of technologically mediated surveillance practice, that is, the degree to which emerging surveillance societies are divergent or convergent in nature. Where the term is used in the singular it suggests a homogenous development of universal surveillance, whereas, we would argue that surveillance is always situated and varied depending on its application in different places—regions, states, cities, etc.—and in the responses and challenges posed by

different cultures, constitutions, legal systems and institutional settings, etc. In this respect, it is more accurate to use the plural version of the term as different societies have different surveillance trajectories and exhibit different surveillance norms—this is a point which is often under-emphasized in academic literature (Murakami Wood 2009; Murakami Wood and Webster 2009). So, although surveillance may have spread as the key 'mode of ordering' in late capitalism we should expect to see different attitudes towards surveillance and different surveillance practices emerging in different countries. This may partly explain why there are divergent approaches to the adoption of CCTV across Europe. For the UK, this would suggest that certain institutional arrangements, norms and attitudes were aligned in such a way that British society was malleable to the rapid diffusion of these systems, whereas in other countries there may have been laws or experiences which meant the provision of CCTV was obstructed (Gras 2004) or more strongly resisted (Samatas 2004). This line of argument can be seen in the work of Bennett and Raab (2006) who develop a comparative perspective in their exploration of the emergence of multiple privacy 'regimes.' At the core of each regime is the idea that they are embedded in, and therefore explained by, their own national setting and history. This is not to suggest that one country is a surveillance society whilst another is not, rather the argument is that all surveillance societies are different—they exhibit different surveillance characteristics and they are different kinds of surveillance societies.

9.5 Concluding Discussion

The landscape of security and liberty in Europe is evolving. Developments arising from the globalization of surveillance, the domestication of security and the emergence of divergent surveillance societies in nation-states are leading to a new 'way of life.' It is certain that in contemporary modern society surveillance is increasingly embedded in everyday life—surveillance is all around us and it is now impossible to exist in modern society without participating in multiple surveillance practices. Often this is done willingly as we seek to support surveillance practices that lead to a safer society with more efficient public services. In this respect, the future of liberty and security is closely intertwined with the deployment of sophisticated technologically mediated surveillance technologies, which are introduced for a variety of purposes, many associated with enhancing the efficiency of public services, but which nevertheless implicitly result in more sophisticated ways of collecting and sharing personal data.

It is evident from the arguments brought forward in this chapter that a key feature of emergent surveillance societies is the centrality of the role played by government and public services. Information-intensive state activity has led to the development of large networked databases, essential to the effective delivery of information age democracy and public services. Furthermore, public policy has played a central role in bringing forward these systems in order to deliver internal

and external security. Public policy and services are therefore inherently intertwined with modern surveillance practices. We would suggest that it is the information intensity of our relations with the state, embedded in and reflected by, the provision of new 'surveillance' technologies that determines and characterizes the nature of modern society and the extent to which this society is dominated by surveillance relations.

A final point which we think is significant is that the normality of living in surveillance societies can result in surveillance activities being accepted without question, even when they are perceived to be undesirable. This is surprising, given the relationship between surveillance, liberty, privacy and personal identity. So, although we are surrounded by technologically mediated surveillance practices and technologies we know relatively little about how surveillance changes our behavior and the institutions around us. Although in this chapter we have demonstrated that surveillance is multi-dimensional—it is subtle, normal, ubiquitous, deep, unobtrusive and powerful—this is not enough, we need to increase and deepen knowledge about living and working in surveillance societies, in order to better understand the consequences of technologically enhanced surveillance, so that citizens and government can be made more aware of the impacts of surveillance and so that the future governance and practice of surveillance can be better informed.

References

Aas K, Gundhus H, Lomell H (eds) (2008) Technologies of InSecurity: the surveillance of everyday life. Routledge, London

Agamben G (2005) State of Exception. University of Chicago Press, Chicago

Andrejevic M (2003) Reality TV: the work of being watched. Rowman and Littlefield, Maryland, USA

Bellamy C, Taylor JA (1998) Governing in the information age. Open University Press, Buckingham

Bennett C, Raab C (2006) The governance of privacy: policy instruments in global perspective. MIT Press, Cambridge

Bigo D, Guild E (eds) (2005) Controlling frontiers: free movement into and within Europe. Ashgate, London

Bunyan T (2005) Unaccountable Europe. Index on censorship, p 3

Coaffee J, Murakami Wood D (2006) Security is coming home: rethinking scale and constructing resilience in the global urban response to terrorist risk. Int Relat 20(4):503–517

Coaffee J, Murakami Wood D, Rogers P (2009) The everyday resilience of the city. Palgrave, Hampshire, UK

Edwards P (1996) The closed world: computers and the politics of discourse in cold war America. MIT Press, Cambridge, MA

Ericson RV (2006) Crime in an insecure world. Polity Press, Cambridge

Garfinkel S (2000) Database nation: The death of privacy in the 21st century. O'Reilly, Sebastopol, CA

Gill M, Spriggs A (2005) Assessing the impacts of CCTV. Home office research study 292. Home Office, UK

Graham S (ed) (2004) Cities, war and terrorism: towards an urban geopolitics. Blackwell, Oxford

Gras M (2004) The legal regulation of CCTV. Eur Surveill Soc 2(2/3):216–229
Groombridge N (2002) Crime control or crime culture TV? Surveill Soc 1(1):30–46
Groombridge N (2008) Stars of CCTV? How the home office wasted millions—a radical treasury/audit commission view. Surveill Soc 5(1):73–80
Haggerty K, Ericson R (2000) The surveillant assemblage. Br J Sociol 51(4):605–622
Hardt M, Negri A (2000) Empire. Harvard University Press, Cambridge, MA
Honess T, Charman E (1992) Closed circuit television in public places: its acceptability and perceived effectiveness. Home office police research group, crime prevention unit (Paper 35). Home Office, UK
Kaldor M (1981) The baroque arsenal. Hill and Wang, New York, USA
Klein N (2008) The shock doctrine: the rise of disaster capitalism. Henry Holt and Co, New York, USA
Lace S (ed) (2005) The glass consumer. Policy Press, Bristol
Law J (1992) Organizing modernity: social order and social theory. Blackwell, Oxford
Lembke J (2002) Competition for technology leadership: EU policy for high technology. Edward Elgar, Cheltenham, UK
Loader I, Walker N (2007) Civilizing security. Cambridge University Press, Cambridge
Lyon D (1994) The electronic eye: the rise of the surveillance society. Polity Press, London
Lyon D (2001) Surveillance society: monitoring everyday life. Open University Press, Milton Keynes
Lyon D (2007) Surveillance studies: an overview. Polity Press, London
MacDonald F (2007) Anti-astropolitik: outer space and the orbit of geography. Prog Human Geogr 31(5):592–615
Matthiessen T (1997) The viewer society: Michel Foucault's 'Panopticon' revisited. Theor Criminol 1(2):215–233
Metz S (2000) Armed conflict in the 21st century: the information revolution and postmodern warfare. Strategic Studies Institute
Monahan T (ed) (2006) Surveillance and security: technological politics and power in everyday life. Routledge, New York
Murakami Wood D (2009) The surveillance society: questions of history, place and culture. Eur J Criminol 6(2):179–194
Murakami Wood D, Webster CWR (2009) Living in surveillance societies: the normalisation of surveillance in Europe and the threat of Britain's bad example. J Contemp Eur Research 5(2):259–273
Murakami Wood D et al (2006) A report on the surveillance society. Information commissioner's office (ICO), UK
Norris C, Armstrong G (1999) The maximum surveillance society: the rise of CCTV. Berg, Oxford
Orwell G (1949) Nineteen eighty-four. Martin Secker and Warburg, London
Palmer G (2003) Discipline and liberty. Manchester University Press, Manchester
Rose N (2000) Government and control. Br J Criminol 40:321–339
Samatas M (2004) Surveillance in Greece: from anti-communism to consumer surveillance. Pella, USA
Schneier B (2008) Schneier on security. Wiley, New York
Smith GJD (2004) Behind the screens: examining constructions of deviance and informal practices among CCTV control room operators in the UK. Surveill Soc 2(2/3):376–395
Smith GJD (2007) Exploring relations between watchers and watched in control(led) systems: strategies and tactics. Surveill Soc 4(4):280–313
STOA (Scientific and technological options assessment sub-committee) (1998) An appraisal of technologies of political control. Directorate general of research: European Parliament
Taylor JA, Lips M, Organ J (2009) Identification practices in government: citizen surveillance and the quest for public service improvement. Identity Inf Soc 1:135–154
Varney SD (2006) Service transformation: a better service for citizens and businesses, a better deal for the tax payer. The Stationary Office, Norwich

Webster CWR (1996) Closed circuit television and governance: the eve of a surveillance age. Inf Infrastruct Policy 5(4):253–263
Webster CWR (2004) The diffusion, regulation and governance of closed-circuit television in the UK. Surveill Soc 2(2/3):230–250
Webster CWR (2009) CCTV policy in the UK: reconsidering the evidence base. Surveill Soc 6(1):10–22
Welsh BC, Farrington DP (2002) Crime prevention effects of CCTV: a systematic review. Home office research study 252. Home Office, UK
Williams CA (2003) Police surveillance and the emergence of CCTV in the 1960s. Crime Prev Community Saf 5(3):27–37
Williams CA (2009) Police filming English streets in 1935: the limits of mediated identification. Surveill Soc 6(1):3–9

Chapter 10
The Evolution of New Technologies of Surveillance in Children's Services in England

Paul Michael Garrett

Abbreviations

ACPO	Association of Chief Police Officers
CAF	Common Assessment Form
CCTV	Closed Circuit Television
CPd	ContactPoint
ECHR	European Convention on Human Rights
EM	Electronic Monitoring
GPS	Global Positioning System
ICO	Information Commissioner's Office
ICT	Information and Communications Technologies
JCHR	Joint Committee on Human Rights
MORI	Ipsos MORI's Social Research Institute
RFID	Radio Frequency Identification

Contents

10.1 Introduction 166
10.2 Thinking about Surveillance 166
10.3 Case Study: ContactPoint 172
10.3.1 A Counter-Productive Move? 174
10.3.2 Opposition 174

Contribution received in 2010.

P. M. Garrett (✉)
Political Science and Sociology, National University of Ireland, Galway, Ireland
e-mail: pm.garrett@nuigalway.ie

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_10,

10.3.3 Implementation 176
10.4 Conclusion 178
References 180

10.1 Introduction

This chapter will particularly focus on how information and communications technologies (ICT) are increasingly central to the 'modernization' of Children's Services in England. Initially, it will discuss what has been termed the 'surveillance society' or—what is preferred here—the 'surveillance state'. The second half of the chapter will examine ContactPoint (CPd): a database which is to contain basic details on all children in England.[1] This 'innovation' has resulted in a good deal of controversy with some viewing the introduction of CPd as eroding the privacy of children and their parents. However, the system began to be introduced, on a phased basis, from January 2009. However, in 2010 the New Labour government was defeated and with the defeat the plan for CPd is likely to have ended.

10.2 Thinking about Surveillance

Surveillance is not, of course, intrinsically repressive, and dominant economic and social forces in society determine how surveillant practices evolve. David Lyon (2001a, p. 2) defines 'surveillance' as 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered.' He goes on to maintain that it is now 'hard to find a place, or an activity, that is shielded or secure from some purposeful tracking, tagging, listening, watching, recording or verification device' (Lyon 2001a, p. 1). For Nik Rose (2000, p. 325) surveillance is now 'designed in' to the flows of everyday existence'. In short, we now live in, what the sociologist Gary T. Marx has referred to as, a 'surveillance society' (Lyon 2001b, p. 32).

> The concept of a surveillance society denotes a situation in which disembodied surveillance has become socially pervasive. The totalitarian fears of Orwellian control all relate to *state* surveillance, whereas the notion of surveillance society indicates that surveillance activities have long spilled over the edges of government bureaucracies to flood every conceivable conduit (Lyon 2001a, p. 33, original emphasis; see also Lyon 2006).

Rose (2000, p. 325) is also of the opinion that 'control is not centralized but dispersed' flowing from 'a network of open circuits that are rhizomatic and not hierarchical'. Part of this analysis suggests that vertical or state surveillance 'still

[1] The UK government has been keen to downplay the fact this scheme is a database—hence the more recent designation Contactpoint—but Capgemini, the multinational corporation responsible for developing the system is less cagey and more plain speaking in its annual report: informing shareholders and other readers that it has succeeded in obtaining a £40 million contract to develop a 'database assembling information on British citizens from birth to 18 years of age' (Capgemini 2007, p. 60).

exists but tends to be less centralized as personal data circulates more and more between public and private (commercial) realms' (Lyon 2001a, p. 33).

Within sociology and criminology, complex debates are, therefore, now taking place which examine whether surveillance is centralized, in the Orwellian sense, or whether the growth of surveillance systems is more dispersed, decentralized, and 'rhizomatic', more 'like a creeping plant than a centrally controlled trunk with spreading branches' (Lyon 2001a, p. 4). However, the idea that surveillance is now diffusing into society at large and is no longer so dominated by the state apparatus is somewhat contentious. Indeed, the perspective developed in this chapter is that the concept of 'Surveillance state' is, perhaps, more convincing (Jameson 2002). This is because, on account of the commencement of an endless 'war on terror', surveillance can be interpreted as actually becoming more 'vertical' (see also Lyon 2003) also, of course, most of the surveillance systems targeted at children, referred to in what follows, are state generated endeavors. Nonetheless, it may be that the main utility of the 'surveillance society' motif is that, it perhaps captures better the sheer omnipresence of surveillant practices in neoliberal societies.

Concerns about surveillance have now spilled over from the discourse of sociology and criminology and into wider civil and public areas. Moreover, such concerns are now even 'officially' recognized and pondered over, with the Information Commissioner's Office (ICO) 2006a which unambiguously maintained that we now 'live in a surveillance society'. It is pointless to talk about surveillance society in the future sense (ICO 2006a, p. 1). The ICO has, however, been keen to stress that the evolution of this 'surveillance society' is not the product of a conspiracy.

> Conventionally, to speak of surveillance society is to invoke something sinister, smacking of dictators and totalitarianism (but it) is better thought of as the outcome of modern organizational practices, businesses, government, and the military than as covert conspiracy (ICO 2006a, p. 1).

Furthermore, some forms of surveillance had 'always existed' (ICO 2006a, p. 1). The ICO report did not directly address the notion that the 'surveillance state' designation may be a more appropriate term and it predictably fails to furnish a political interpretation of some of the key factors leading to the new prominence of surveillance. However, substantial parts of the report remain important for those in Children's Services, and elsewhere in the public sector, because of the methodical way it goes about identifying some of the main processes and issues.

For example, in a section of the report analyzing the context for the 'surveillance society', it focuses on three elements. First, a preoccupation, in England—and elsewhere—with *risk and security* having given rise to a '*pre-emptive* as opposed to a *preventative* approach to risk' (ICO 2006a, p. 11, original emphases). As a result, it is maintained, current and 'emerging practices feature technologies and data-mining to this end'. Significantly also, 'pre-emptive risk profiling shifts surveillance practices toward the screening of the actions and transactions of the general population' (ICO 2006a, p. 11). Also influential, for the authors of the report, is the rise of epidemiology and the modeling associated with medical surveillance. For instance, the monitoring and tracking of individual disease cases,

recording occurrences of disease for statistical analysis, screening whole populations to identify individuals or groups at higher than average risk for a disease. Indeed, this notion is important because, it might also be argued that this orientation may be impacting on prevention strategies and practices which are intent on 'targeting' those children 'at risk' of becoming criminal or 'anti-social'.

A second factor having an impact on the way the 'surveillance society' is evolving, is referred to as the militarization of surveillance and the 'complex interaction between military and economic logics' (ICO 2006a, p. 14). The report, also notes the way which many 'surveillance technology companies are intimately bound up with the military, yet sell increasingly to civilian users' (ICO 2006a, p. 14). Related to this contextual dynamic, is the 'increasingly military way of talking about everyday safety' (ICO 2006a, p. 14): for example, the 'war on drug,' 'war on crime' and so on (see also Beckett 2003). Finally, the growth of elective 'personal information economies' may also be a significant: for example, some people's willingness to use, for example, 'MySpace', 'Bebo', and 'Facebook' may be serving to domesticate surveillance technologies. In this context, Boyne (2000, p. 292) has referred to what he perceives as the 'relative calm with which contemporary developments of surveillance powers have been received'. Numerous 'reality TV' shows, such as Big Brother, may also have helped domesticate certain modes of surveillance, such as CCTV.

The ICO usefully differentiates some of the main surveillance technologies. These include telecommunications, video surveillance, the database, biometrics and locating, tracking, and tagging technologies. Indeed, all of these technologies are increasingly being deployed in within Children's Services and other areas of social work and social care provision. Technologies concerned with electronic monitoring (EM), particularly tagging, for example, are increasingly prevalent. The Criminal Justice Act 1991 legislated for EM for those on curfew orders and in 1999, EM curfews became a national scheme. The Criminal Justice and Court Services Act 2000 introduced EM for young offenders (as a component in bail, community sentences, and post-custody supervision). Significantly, and gelling with the politics of neoliberalism, England and Wales are the only European countries 'to use the private sector to deliver EM' (Nellis 2005, p. 170).

Increasingly satellite tracking is also beginning to play a significant a role in EM: global positioning system (GPS) technology was used, on a pilot basis, in September 2004. This 'targeted' sex offenders, domestic violence offenders and persistent offenders. Providing a good example of technological 'functions creep', the following month it was extended to cover 'failed' asylum seekers—those awaiting deportation. This was the 'first use of EM in England outside a criminal justice setting' (Nellis 2005, p. 172). Private employers, however, are now deploying a variety of wearable devices for staff in the wholesale distribution industry.

> [Some] consist of computers worn on the arm and finger computers to local area radio networks and to GPS systems... These devices calculate how long it takes to go from one part of the warehouse to the other and what breaks the workers need and how long they need to get to the toilet. Any deviation from these times is not tolerated (GMB 2005).

Moreover, attention is now being given to the potential of using micro-chip technology to monitor an array of 'problem populations'. Early in 2008, for example, it was reported that ministers, in England, were even considering implanting 'machine readable' microchips under the skin of thousands of offenders, in the community, because this could create more prison space. Radio frequency identification (RFID) microchips would be surgically inserted under the skin and this would carry scannable personal information, including offending record. Such a move would be in line with a proposal from the Association of Chief Police Officers (ACPO) that electronic chips should be surgically implanted into convicted pedophiles and sex offenders to alert authorities if they are in the environs of 'forbidden zones' such as schools, playgrounds, and former victim's homes. These devices (already used to keep a track of dogs, cats, and cattle) would be injected into the arm of an offender.[2] In terms of social 'care,' the Alzheimer's Society is of the view that satellite tracking systems could help families care for patients longer at home: a move opposed, in fact, by the National Pensioners' Convention.[3] In the US, one of the market leaders in RFID technology is VeriChip and its RFID devices are now being inserted into the bodies of people suffering from Alzheimer's disease and related conditions (see VeriChip 2007).

Given the concentration of this chapter on the creation of CPd, the evolution of database technologies is, perhaps, particularly important (Anderson et al. 2009; see also Elmer 2004). Indeed, databases are now playing a key role throughout public services and are also more central in relation to policing and crime detection; for example, 40% of black males are profiled on the National DNA Database. It has also been reported that nearly 1.5 million 10–18 year-olds will have been entered by 2009.[4] Meanwhile, the director of forensic services at New Scotland Yard and spokesman for ACPO has argued that all school children at risk of becoming criminals should be entered onto the National DNA Database (Graef 2008).

Significantly also, multiple data can now be gathered, tabulated, and cross-referenced far faster than with, what is now termed, 'old-fashioned twentieth century paper documents' that were once a characteristic of bureaucracy (Home Office Border and Immigration Agency 2008, p. 4). These developments have, moreover, led some to stress the concept of 'dataveillance'.

> [A] variation of surveillance [which] emphasizes the importance of databases, rather than visual or auditory means of watching over people, in the practices of states and companies' (ICO 2006a, p. 20).

For the ICO, there are also a number of issues of concern about surveillance which remain highly relevant for Children's Services. First, there is the risk of technical synergy and function creep with information 'gathered for one purpose or in one domain' leaking through into others (ICO 2006a, p. 26). Second, there is

---

[2] See also Prisoners 'to be chipped like dogs' 2008.

[3] Electronic tags to track dementia patients 2007.

[4] See DNA register 'labels children criminal' 2008.

a need to be wary about a drift toward pervasive surveillance with surveillance practices becoming 'ubiquitous, taken for granted, and largely invisible' (ICO 2006a, p. 27). Indeed, as Didier Bigo (Bigo 2006) as remarked, after.

> [A] while, these technologies are considered so banal (such as ID checks in many countries... and biometric identifiers in documents), that nobody (including the judges) asks for proof of their legitimacy and their efficiency after a period of time.

Third, there is an urgent need to be alert to the limits of technology given that the promise of technologies, often delivered by corporations intent on developing new markets or safeguarding and maintaining existing markets, 'is almost never quite delivered as anticipated' (ICO 2006a, p. 28). Finally, the ICO report reminds its readers of the dangers of technological lock-in and regulatory lag. Once again, moreover, important points are made in relation to the potential problems which could result for children and related services.

> Surveillance is the first port of call in response to any kind of problem is a strongly managerialist solution, frequently proposed to governments by management consultants who operate on measurement-based world views... However, the more that states, organizations, communities and people become dependent on surveillance technologies, the more there is apparent "lock-in" which prevents other options from being considered, and a comprehension gap which increases a dependence on expertise outside the democratic system (ICO 2006a, pp. 29–30).

Turning to examine surveillance processes, the ICO suggests that one of the 'most significant developments is how surveillance, that was once reserved for the "suspect" or "deviant", has become extended to cover the majority of the population, which can then be sorted, categorized, and targeted' (ICO 2006a, p. 30). Specific processes related to 'information sharing' and 'joined up' systems might also give rise to public concern—despite the centrality of such themes and practices to New Labor 'modernization'—because one.

> [E]ffect of this key development is that the boundaries that were once thought to have provided certain, albeit fragile, safeguards to privacy and limits to surveillance are called into question, often leaving both the public and the service-providers bewildered about how personal information is, and should be, managed. Personal data flow into new channels—some of them private—through organizations that never before had access to them, and whose traditions of confidentiality and privacy protection may differ substantially from each other, and from those agencies in the public sector (ICO 2006a, p. 34).

In general, therefore, the Information Commissioner is explicitly and lucidly mindful of a constellation of complex issues and problems which are detectable within public services and which are impacting on Children's Services during a period of 'modernization' where ICT is fulfilling an increasingly central role. His report is also an alert to some of the adverse social consequences of surveillance: discrimination, for example 'in the form of differential speed, ease of access, and various degrees of social exclusion, is a major outcome of the social sorting processes produced by surveillance (ICO 2006a, p. 43). Moreover, there are fundamental questions (concerning democracy, accountability, and transparency) which are raised by the surveillance. In policy terms it is proposed, therefore,

Table 10.1 The major databases collecting personal information on children in England

Scheme	Contents
ASSET	Used by youth offenders' teams, youth inclusion and support panels and youth courts: features profiles of young offenders for the purpose of sentencing and rehabilitation
Centrally devised assessment schedules used by local authorities: materials associated with LAC; the AF; the CAF/eCAF	Children/young people in contact receiving local authorities: which specific templates are used is determined by how the child/young person is classified
Connexion's Customer Information Service (CCIS) and Connexions Card	Information on all 13–19 year-olds. Smart Card for 16–19 year-olds operated by private company Capita which is enabled to carry out consumer profiles.
ContactPoint (CPd)	To contain basic details on children (and some adults up to 25 years-old).
DNA Database	Nearly 1.5 million 10–18 year-olds will have been entered by 2009. ACPO seeking even more extensive use.
Fingerprinting for access to services and facilities	A number of local education authorities compile biometric information on children in the form of fingerprints e.g. to enable children to access libraries
Integrated Children's System (ICS)	An 'electronic social care record' for children: continues to be 'rolled out' nationally. Aims to store and analyze personal details on children in contact with Children's Services.
'Lost pupil' databases	Data on children not currently in state education in England
MERLIN	Used by the Metropolitan Police: records information on children 'coming to notice' (CTN) of the police. Some other constabularies use similar systems.
National Pupil Database (NPD)	Extensive factual details on every child in state education in England
National Register of Unaccompanied Children (NRUC)	Promoted by the Association of London Government: used to exchange information between local authorities and the Immigration and Nationality Directorate (IND) on unaccompanied under 18 asylum seekers; used to manage funding and to respond to concerns about asylum seekers giving false ages
NOTIFY	Used by Greater London Authority and London boroughs: records information on the movement of homeless households
ONSET	Same as ASSET but for those not convicted: also used to try and identify those thought likely to offend

(continued)

Table 10.1 (continued)

Scheme	Contents
RAISEonline (Reporting and Analysis for Improvement through School self-Evaluation	System for analyzing data in the NPD
RYOGENS	Produced by private company Esprit and deployed by a number of local authorities: logs 'concerns' about children and young people regarded as 'vulnerable'

This Table is partly derived from information produced by the Information Commissioner's Office (ICO) in November 2006 (ICO 2006b). It does not purport to be exhaustive. It is also featured in Garrett (2009a)

that 'surveillance impact assessments' should be produced before any proposed 'reform' is introduced (ICO 2006a, pp. 93–95). Indeed, it is vital to recognize that surveillance has a differential impact. Clearly, no one evades surveillance although some surveillant practices intrude into certain lives more emphatically than they do in others. In this context, children are 'arguably more hemmed in by surveillance and social regulation than ever before' (James and James 2001). Table 10.1, therefore, attempts to identify some of the major databases concerned with children (see also Garrett 1999, 2003, pp. 145–148; Garrett 2005).

In what follows, the aim is to provide a concise critical commentary charting the evolution of one particular database, the CPd: a scheme which will, it has been maintained, result in the 'virtual electronic tagging of families' (BAAF 2004) and even risk becoming a 'search engine for pedophiles' (Carvel 2004).

10.3 Case Study: ContactPoint

In autumn 2003, the government published Every Child Matters (ECM), its plan for re-organizing services for children (Chief Secretary to the Treasury, 2003). Whilst New Labor's vision for change was broadly welcomed by child welfare professionals and others, the idea of introducing—what was referred to at the time as—'local information hubs', an electronic system to facilitate the collating and sharing of information about children, was viewed much less favorably. ECM stated the aim was that, in localities, the 'hub' would consist of 'a list of all the children living' in the area and other 'basic details'.

- Name, address, and date of birth.
- School attended or if excluded or refused access.
- GP.
- A 'flag' stating whether the child is known to agencies such as education welfare, social services, police, and youth offending teams, and if so, the contact details of the professional dealing with the case.

- Where a child is known to more than one specialist agency, the lead professional who takes overall responsibility for the case.

It was also stated that these envisaged 'information systems' would 'be based on national data standards to enable the exchange of information between local authorities and partner agencies, and be capable of interacting with other data sets' (Chief Secretary to the Treasury 2003, p. 53). A 'lead professional' would act as 'gatekeeper' for this information sharing system and in order to indicate that there were concerns about a child or family, readers of ECM were advised.

> [T]here is a strong case for giving practitioners the ability to flag on the system early warnings when they have concern about a child which in itself may not trigger or meet the usual thresholds for intervention. The decision to place such a flag of concern on a child's record, which may be picked up by another agency making a similar judgement, lies with the practitioners... [W]e are consulting on the circumstances (in addition to child protection and youth offending) under which information about a child could or must be shared, for preventative purposes, without the consent of the child or their carers. We would also welcome views on whether warning signs should reflect factors within the family such as imprisonment, domestic violence, mental health or substance misuse problems amongst parents and carers (Chief Secretary to the Treasury 2003, pp. 53–54).

As early as 2003, therefore, it was apparent that the envisaged system would result in more information being collated on children and potentially more 'tracking' taking place. Equally important, at this foundational stage, there were a number of key omissions. Would, for example, the police be able to access the databases and seek out data when investigating matters unrelated to children, but connected to other facets of criminal detection or intelligence? Would the Immigration Service be able to access the hubs when determining if an individual or family has the right to remain in the England? Were there dangers of (external and internal) hacking or misuse? However, it was, perhaps, the notion of 'flags of concern' which appeared to be the most concerned and ill-conceived.

At this stage it was also left unclear when a 'flag of concern' would be electronically placed on a child's personal database. Indeed, it appeared that the government's plan left far too much room for the discretion of individual practitioners about when 'thresholds' may have been crossed. Other aspects of the plans indicated that there were likely to be substantial civil liberties concerns. It was also unclear if a child, young person, or parent would be informed that a 'professional' had electronically inserted a 'flag of concern' on a computer database. Neither was there any information provided about how these 'flags' would be treated when a young person reached 18 years old. As is clear from the extract from ECM, referred to earlier, the government also seemed intent on expanding categories in order to insert 'warning signs' where there were instances of 'imprisonment, domestic violence, mental health or substance misuse problems amongst parents and carers'. In short, a mixture of hardships and woes, some of which may not always result in child protection concerns.

10.3.1 A Counter-Productive Move?

Furthermore, some felt that this plan, featured in ECM, could be dangerously counter-productive because it could deter a hard-pressed family from seeking out help and support because they might be fearful of their private information being placed on the electronic 'hub.' Perhaps also social class location can be connected to concerns that some children and parents might be deterred from seeking out help because they are fearful that their 'details' will be entered onto a database. MORI, for example, undertook research on public awareness and perceptions of privacy and data sharing for the Department of Constitutional Affairs in 2003. Extraordinarily given the government's plans for accumulating and sharing information on over 11 million children, only the views of those aged 15 and over were sought. However, 60% of those asked stated that they were 'very or fairly concerned' about public services sharing their personal information, with 22% '*very* concerned.' Only 12% stated that they were 'not at all concerned' (Skinner et al. 2003, original emphasis). These percentages reflect the public's wariness about privacy being undermined by electronic 'information sharing,' but also of note is the fact that a 'fairly consistent trend' is for the middle social classes to be least concerned (Skinner et al. 2003, p. 5). Related to this, those in 'the middle social classes are more likely to trust public services to handle information responsibly than working class people/those on benefits' (Skinner et al. 2003, p. 21).[5] It could be argued, therefore, that the setting up of databases might particularly deter working class children and parents from seeking out help.

Additionally—and reflecting some of the thinking contained in the ICO report referred to earlier—it was felt, by some commentators, that the belief in an enhanced electronic monitoring system risked being perceived as something of a 'panacea' which would 'solve' a panoply of highly complex social problems relating to children and their families (Winchester 2003). More generally, in fact, it could be maintained that this simplistic orientation is detectable across the literature associated with 'e-government' agenda for Children's Services.

10.3.2 Opposition

Following the publication of ECM, criticisms of the plan for databases were voiced not only from children's rights groups, but from a range of diverse organizations. The civil liberties group, Liberty, expressed concern about the privacy of children and families being undermined and the British Medical Association was fearful that the envisaged scheme risk breaching doctor-patient confidentiality. Moreover, upon publication of the Children's Bill, the parliamentary Joint Committee on Human Rights (JCHR) went on to express serious concerns about

[5] See also ID cards may put poorer people at risk of fraud 2008.

the proposed databases (JCHR 2004). More specifically, the JCHR felt that the information sharing provisions in the Bill involved 'serious interference' with Article 8 of the European Convention on Human Rights (ECHR), which seeks to ensure respect for private life. Related to this, it was maintained that the government was failing to provide evidence that this interference was proportionate and justified under Article 8 (2) of the ECHR (JCHR 2004, pp. 29–35). The JCHR was, moreover, concerned about the 'breadth of the regulation-making powers being conferred on the Secretary of State' (JCHR 2004, p. 32). In this context, the government simply maintained that it needed to retain 'flexibility to develop the databases in light of the experiences of the current pilot projects being carried out and technical advice commissioned but not yet delivered' (JCHR 2004, p. 32). Given this position, the JCHR reasonably maintained that parliament was 'being asked to authorize in advance a major interference with Article 8, rights without evidence demonstrating its necessity being available' (JCHR 2004, p. 32). Importantly also, the measured report from the JCHR asserted:

> Maintaining a child protection register, or even a register of children "in need" and therefore in receipt of Children Act assistance from the local authority, is a much more targeted measure aimed at protecting vulnerable children. But a universal database seems to us to be rather more difficult to justify in Article 8 terms. Adults are also the beneficiaries of universal services such as health care and other services, such as community care, for which they may be eligible in certain circumstances. It appears to us that the strict logic of the Government's position is that it would be justifiable interference with adults' Article 8 rights to maintain a similar database of all adults in the UK in order to ensure that those amongst them who are or may be entitled to receive certain services from the state actually receive them (JCHR 2004, p. 33).

Within parliament, substantial opposition was provided within the unelected upper chamber, the House of Lords: more specifically, a core group of well-briefed, Conservative and Liberal Democratic members deployed a number of arguments which endeavored to undermine the scheme, its envisaged purpose and day-to-day operation. This was, perhaps, most apparent in the House of Lords' Committee Stage debate of the Children Bill in May 2004. For the Lords, plans for the databases were vague on a number of key points. Indeed, it was asserted that 'the whole thing is ill-formed' and 'wishy-washy' and the government had difficulties in trying to rebut this charge (see the comments of Earl of Northesk).[6] The lack of definition and skeletal nature of the legal framework, which had been provided for the databases, was targeted for particular criticism. Critics maintained, for example, that the Children Bill delegated exceedingly wide powers to the Secretary of State, permitting him/her to 'establish and operate databases' with regulations setting out the operational details.

[6] Lord's Hansard, 24 May 2004, col. 1159. All future references to the contributions in the House of Lords' Commitee Stage debate of the Children Bill in May 2004 will simply provide the name of the contributor and the relevant column (col.) in the House of Lords' Hansard report.

The government's chief spokesperson in the Lords argued, without referring to any evidence, that information needed to be electronically logged because 'time and again, professionals cannot act on ... early concerns because they do not know who else is involved' (Baroness Ashton, col. 1095). What was being proposed, therefore, was merely an electronic 'telephone directory', a 'yellow pages' to facilitate the work of busy child welfare professionals. Importantly, for the government, the envisaged databases would, moreover, contain nothing that 'would constitute opinion about any child' (Baroness Ashton, col. 1097). In short, according to the government's rather bland presentation of the issue, all that was being proposed was a rational and technical solution to a perceived social problem.

In some respects, the claim that the envisaged databases could be perceived as a sensible measure is convincing. In broad terms it seems sensible, of course, for Children's Services to continue to exchange relevant information. As mentioned earlier, the policy aspiration to utilize ICT to facilitate such exchanges, fits neatly alongside the endeavor to 'modernize' Children's Services. Moreover, the plan for the databases and the 'wiring up' of these services gels with the notion of 'joined up thinking' (Ling 2002). Furthermore, ideas about 'preventative' action to respond to children 'at risk' of 'abuse' or (somewhat more ambiguously) 'social exclusion' can have a 'common sense' appeal to child welfare professionals and to the wider public. However, as was observed in the House of Lords, when concerted attempts were made to clarify the purpose and scope of the government's plans, we:

> [H]ave here what is potentially a very large-scale system of data recording by the state on its citizens. The system is to be set up in the name of improving the welfare of all children. The names and key personal details of all 11 million children in England are to be recorded for access by professionals from a wide variety of disciplines. The vast majority of children so recorded will not be at risk of suffering significant harm or anything approaching it ... [H]ow can we not regard this mammoth information gathering and information sharing exercise as anything other than grossly intrusive on the privacy of families? (Earl Howe, col. 1154).

10.3.3 Implementation

The New Labour administration was keen to try, via regulations and protocol, to blunt criticism. Consequently, a number of changes were made relating to the operation of the CPd. However, unfortunately for the government and senior local government officers wanting to press ahead with implementation, a whole series of mishaps, even scandals, connected to the 'loss' of government electronic data occurred in 2007 and 2008. This included the disappearance 'in the post' of HM Revenue and Customs, discs containing the personal records of 25 million individuals, including their dates of birth, addresses, bank accounts, and national insurance numbers; also 'lost' were the personal details relating to 7.25 million families in receipt of child benefits. Subsequently, it was reported that the personal details of approximately 3 million learner drivers have been 'lost' by a contractor

in the US state of Iowa.[7] In the summer of 2008 it was then reported that PA Consulting, the consultancy firm involved in the development of national identity cards, had been responsible for losing a memory stick containing the details of all of the 84,000 prisoners in England and Wales.[8] Unsurprisingly these events, as well as illuminating one of the potential pitfalls associated with neoliberal inspired 'outsourcing' or 'contracting out' of core government tasks and functions, led to renewed criticism that storing the personal details of 11 million children on the envisaged CPd was an inherently 'risky' business. More emphatically, this was a reckless 'reform' of Children's Services which could still be avoided.[9]

The New Labour administration remained intent on introducing the CPd. The aim of the administration defeated in the 2010 election was to set up a national system, but the data was to be partitioned into 150 compartments, each relating to a different local authority. The government was, however, remained sensitive to the criticisms which had been deployed since the database plan was first mooted. For example, the 'flags of concern' idea was been abandoned but the scheme was to alert practitioners if a 'common assessment form' (CAF) had been completed on a child. Thus, a CAF symbol or icon would replace a 'flag' when CPd began to fully function on a national basis.

Clearly, an indication as to whether or not a CAF has been completed on a child is preferable to the 'flag of concern' icon which was envisaged initially: for example, the deployment of the latter might have been perceived as inappropriately dramatic. What is more, on a more abstract level, the flag idea can be read as problematic because a flag is a universal signifier of national belonging. Thus, it might be interpreted as fusing issues related to immigration status and child welfare (Sales 2002). In this context, therefore, a CAF symbol extinguishes this particular unease associated with the 'flag of concern'. However, there are also problems connected to the use of the CAF assessments. As Sue White and her colleagues have highlighted here the chief problem appears to be the descriptive, stylistic and interpretive demands it places on practitioners in child welfare (see also White et al. 2008; see also Pithouse et al. 2009).

Fundamentally, though, the outgoing government appeared not to have given in ground in terms of the core and problematic conceptual underpinning of the database plan. Hence, the defensive emphasis on how the 'security' of the CPd would be safeguarded and how access and use would be established and policed. Thus, the presentation switched from seeking to provide a rationale for the CPd to 'making the CPd work' (Ofsted 2007) and stressing that there will only be 'authorised users', within each locality, aided by 'specialist teams' with technical 'know–how'. In this way the New Labour administration were intent on

[7] See 333,000 users to have access to database of english children 2007; Lost in the post—25 million at risk after discs go missing 2007; Personal details of millions of learner drivers lost by contractor in Iowa 2007.

[8] See ID contractor denounced over data lose 2008.

[9] See Security fears prompt call for the scrapping of children's database 2007.

'technologising' a 'politically contested issue, by translating the issue into technical and "common sense" understandings' that served to depoliticise' the CPd project (Penna 2005, p. 145).

10.4 Conclusion

This chapter has not tried to promote a technophobic perspective. Indeed, it must be conceded that ICT have many potential beneficial uses for both practitioners and users within Children's Services. Databases, for example, are a useful 'tool' which can help in the collating and storage of information. The internet also provides many interesting possibilities for child care social work and more politically, for social movements seeking to combat neoliberalism and to champion a more 'democratic technics' (May 2002, pp. 29–32). However, there is also a need to be alert to the ideological atmosphere in which social workers and others in Children's Services perform their new technological role (see, for example, Wacquant 2009). Following Adorno's (2003, p. 118) lead, there is a need to try and ascertain how the technology is imbricated 'within the relations that embrace it.' Moreover, assessment 'tools' devised for intervention are often underpinned, in part, by the functional aspiration to police the socially marginalized (Garrett 2003). Perhaps sensitive to some of the changes impacting on direct-work with children and families, British Association for Fostering and Adoption (BAAF 2004, p. 24) has called for the restoration of what it dubs 'people-focussed social work'. This, moreover, is a theme which has been referred to in some of the debates generated on contemporary social work practices following the death of 'Baby Peter' (Ofsted, Healthcare Commission, HMC, 2008).[10]

Certainly the technological basis for engagement with children and families is changing and with it, the function of practitioners (UNISON 2008; see also Garrett 2009b). More fundamentally, there cannot, of course, be any return to the type of work practices elaborated on the basis of technological and social circumstances that no longer exist. In terms of the near-future, however, the future of the CPd is not assured. The Conservative Party (2009, p. 1), in opposition, pledged to scrap the CPd. It also proposed that 'privacy impact assessments' (PIAs)—favored as we

[10] 'Baby Peter,' a 17-month-old boy, died in August 2007 from severe injuries inflicted whilst he was in the care of his mother, her 'boyfriend' and a lodger in the household. In November 2008 two men were found guilty of causing or allowing the death of a child or vulnerable person. The mother had already pleaded guilty to the same charge. Importantly, for Children's Services, 'Baby Peter' had been subject to a child protection plan following concerns that he had been abused and neglected. Following the convictions, the death of 'Baby Peter, the inadequate responses of child welfare professionals, began to dominate political and media discourses (see Garrett 2009c).

have seen by the ICO—should be triggered in respect of any proposals for new legislation or other measures which involve data collection or sharing. To-date England lacks the robust data protection legislation available in some other jurisdictions; most notably, the Federal Republic of Germany which has, perhaps mainly for historical political and social reasons, the strongest protection for personal data in Europe. Outside of Europe, a number of jurisdictions—for example, Canada, New Zealand and the United States—have also introduced mandatory PIAs (House of Lords Select Committee on the Constitution 2009, p. 71).

Beyond the domain of party politics, there would now seem to be embedded, concerns amongst academics, pressure groups about the evolving surveillant practices of the state, into the lives of citizens (Clark and McGhee 2008; Anderson et al. 2009; House of Lords Select Committee on the Constitution 2009). Importantly also within Children's Services, and related areas of practice, pressures on 'professionals to weaken' the 'right to privacy, autonomy, and confidentiality' are increasingly being driven by market considerations' (Bisman 2008, p. 29). This remark is surely correct, yet there is, perhaps, a failure to interrogate how technologies being deployed across social work, social care, and health fields, in various jurisdictions, are commodities which are marketed and sold by multinational IT corporations. Indeed, this dimension tends to be occluded in most accounts of the 'surveillance society' and how the evolution of this emergent social formation impacts on Children's Services and associated fields. However, the role of the private sector and a more encompassing neoliberal policies—finding expression in privatization and marketization—are surely central. For example, the UK 'spends over £16 billion a year on IT' (Anderson et al. 2009, p. 4); related to this '£500 million of public money was invested in CCTV in the decade up to 2006' (House of Lords Select Committee on the Constitution 2009, p. 20). However, the role of the private sector has perhaps remained shadowed, hidden or undeveloped in, for example, many academic contributions to debates on the deployment of new surveillance technologies. Nonetheless, the private sector has been central in terms of 'selling' the idea that governments and local authorities need to evolve in new ways of governing and of managing information and 'joining up' services (Ling 2002). Moreover, the more extensive use of corporate management consultants has also provided something of an 'opening' for companies to insert their upbeat 'vision' of the 'e-society'. More prosaically, of course, the introduction of the most sophisticated computer technologies—particularly in the form of databases—has tended to be deployed to classify the users of services so as to restrict, limit, and ration access to services.

The election of a new government in Britain, in May 2010, has done little so far to alleviate concerns. The coalition Conservative/Liberal Democrat administration is now committed to 'scrapping' CPd 'as soon as possible' and it is 'considering its replacement with an alternative approach to support vulnerable children' (Department of Education 2010; see also Garboden 2010). However, more generally, concerns about the evolution of a 'surveillance society' have not been dispelled. The current Information Commissioner (ICO 2010), for example, is

pressing ministers for new privacy safeguards in the wake of a report which suggests that moves towards a surveillance society are, in fact, expanding and intensifying.

References

333,000 users to have access to database of english children (2007) The Guardian, 18 June, p 12

Adorno TW (2003) Can one live after auschwitz: a philosophical reader. Stanford University Press, USA

Anderson R et al (2009) Database state. Joseph Rowntree Reform Trust, York

BAAF (British Association for Fostering and Adoption) (2004) Information, referral and tracking—the professional basis for informed judgement: extract from BAAF's response to every child matters. BAAF, London

Beckett C (2003) The language of siege: military metaphors in the spoken language of social work. Br J Soc Work 33(5):625–639

Bigo D (2006) Security, exception, ban and surveillance. In: Lyon D (ed) Theorizing surveillance. Willan, Devon, pp 46–69

Bisman C (2008) Professional confidentiality revisited: personal information and the professional relationship. In: Clark C, McGhee J (eds) Private and confidential? handling personal information in social and health services. Policy Press, Bristol, pp 17–35

Boyne R (2000) Post-panopticism. Econom Soc 29(2):285–307

Capgemini (2007) Annual report. http://www.capgemini.com/annual-report/2007/index.php?zPg=pdf/version-pdf/pdf_en/version-pdfEN&zPx=html&langue=en

Carvel J (2004) All eyes on the child. The guardian society, children's services supplement, 19 May, pp 2–3

Chief Secretary to the Treasury (2003) Every child matters. HMSO, Cm 5860, London

Clark C, McGhee J (eds) (2008) Private and confidential? handling personal information in social and health services. Policy Press, Bristol

Conservative party (2009) Reversing the rise of the surveillance state. http://www.conservatives.com/News/News_stories/2009/09/~/media/Files/Policy%20Documents/Surveillance%20State.ashx

Department of Education (2010) Review of child protection: better frontline services to protect children. Press notice, 10 June. http://www.education.gov.uk/news/press-notices-new/reviewofchildprotection

DNA register 'labels children criminal' (2008) The observer, p 4

Electronic tags to track dementia patients (2007) The Times, 27 December

Elmer G (2004) Profiling Machines. MIT, Massachusetts

Garboden M (2010) Facebook-style site in bid to replace ContactPoint. Community care, 19 August. http://www.communitycare.co.uk/Articles/2010/08/19/115106/facebook-style-site-in-bid-to-replace-ContactPoint.htm

Garrett PM (1999) Producing the moral citizen: the looking after children' system and the regulation of children and young people in public care. Crit Soc Pol 19(3):291–312

Garrett PM (2003) Remaking social work with children and families: a critical discussion on the 'modernisation' of social care. Routledge, London

Garrett PM (2005) Social work's 'electronic turn': notes on the deployment of information and communication technologies in social work with children and families. Crit Soc Pol 25(4):529–554

Garrett PM (2009a) 'Transforming' children's services? social work, neoliberalism and the 'modern' world. McGraw Hill/Open University, Maidenhead

Garrett PM (2009b) Marx and 'modernization': reading capital as social critique and inspiration for social work resistance to neoliberalization. J Soc Work 9(2):199–221

Garrett PM (2009c) The case of 'Baby P': opening up spaces for debate on the 'transformation' of children's services. Crit Soc Pol 29(3):533–547
GMB (2005) GMB congress demands end to electronic tagging of workers 'battery farm' workplaces. Press release, 6 June. http://www.gmb.org.uk/Templates/Internal.asp?/NodalID=91861
Graef R (2008) The usual suspects. The Guardian, 21 March, p 42
Home Office Border and Immigration Agency (2008) Introducing compulsory identity cards for foreign nationals. Home Office, London
House of Lords Select Committee on the Constitution (2009) Surveillance: citizens and the state. Stationery Office, London
ID cards may put poorer people at risk of fraud (2008) The Guardian, 16 May, p 11
ID contractor denounced over data lose (2008) The Guardian, 23 August
Information Commissioner's Office (ICO) (2006a) A report on the surveillance society: for the information commissioner by the surveillance studies network. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf
Information Commissioner's Office (ICO) (2006b) protecting children's personal information: ICO issues paper, 22 November 2006. http://www.ico.gov.uk/upload/documents/pressreleases/2006/protecting_childrens_personal_information.pdf
Information Commissioner's Office (ICO) (2010) information commissioner's report to parliament on the state of surveillance. http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/surveillance_report_for_home_select_committee.ashx
James AL, James A (2001) Tightening the net: children, community and control. Br J Sociol 52(2):211–228
Jameson F (2002) The dialectics of disaster. S Atl Q 101(2):197–305
JCHR (House of Lords and House of Commons Joint Committee on Human Rights) (2004) Children bill: nineteenth report of the session 2003–2004. Stationery Office, London
Ling T (2002) Delivering joined-up government in the UK: dimensions, issues and problems. Public Adm 80(4):615–642
Lost in the post—25 million at risk after discs go missing (2007) The Guardian, 21 November, p 1
Lyon D (2001a) Surveillance society: monitoring everyday life. Open University, Buckingham
Lyon D (2001b) Surveillance after September 11. Sociological research online 6 (3). http://www.socresonline.org.uk/6/3/lyon.html
Lyon D (2003) Surveillance after September 11. Polity Press, Cambridge
Lyon D (ed) (2006) Theorizing surveillance. Willan, Devon
May C (2002) The information society. Polity, Cambridge
Nellis M (2005) Electronic monitoring, satellite tracking, and the new punitiveness in England and Wales. In: Pratt J et al (eds) The new punitiveness: trends theories and perspectives. Willan, Devon, pp 167–189
Ofsted (2007) Making contactpoint work. http://www.ico.gov.uk/upload/documents/pressreleases/2006/protecting_childrens_personal_information.pdf
Ofsted, Healthcare Commission, HMC (2008) Joint area review: haringey children's services authority area. http://www.ofsted.gov.uk/oxcare_providers/la_download/(id)/4657/(as)/JAR/jar_2008_309_fr.pdf
Penna S (2005) The children act 2004: child protection and social surveillance. J Soc Welf Fam Law 27(2):143–157
Personal details of millions of learner drivers lost by contractor in Iowa (2007) The Guardian, 18 December, p 4
Pithouse A et al (2009) A tale of two CAFs: the impact of the electronic common assessment framework. Br J Soc Work, Advanced access from 25th February. http://bjsw.oxfordjournals.org/
Prisoners 'to be chipped like dogs' (2008) The independent on Sunday, 13 January, pp 1–4
Rose N (2000) Government and control. Br J Criminol 40:321–339

Sales R (2002) The deserving and undeserving? refugees, asylum seekers and welfare in Britain. Crit Soc Policy 22(3):456–479

Security fears prompt call for the scrapping of children's database (2007) The Guardian, 6 December, p 10

Skinner G, Tonsager AM, Hall N (2003) Privacy and data-sharing: survey of public awareness and perceptions. MORI, London

UNISON (2008) Progress report on safeguarding: UNISON memorandum of lord laming. London, UNISON. http://www.unison.org.uk/acrobat/B4364a.pdf

VeriChip (2007) VeriChip corporation partners with alzheimer's community care. Press release, 22 February. http://www.verichipcorp/news/1172151146

Wacquant L (2009) Punishing the poor: the neoliberal government of social insecurity. Duke University, Durham

White S, Hall C, Peckover S (2008) The descriptive tyranny of the common assessment framework: technologies of categorization and professional practice in child welfare. Br J Soc Work. Advanced electronic access from 16 April 2008. http://bjsw.oxfordjournals.org/

Winchester R (2003) Welcome to the machine. community care, October 30–5 November, pp 26–28

Chapter 11
Electronic Child Records in The Netherlands: A Legitimate Path to Right Wrongs?

Simone van der Hof

Contents

11.1 Introduction 183
11.2 Social Paradigms 184
11.3 From Simple Records to a Pervasive Monitoring System 185
11.4 The Potential Impact of ECRs 188
11.5 Legal Assessment I: A Human Rights-Based Approach 190
11.6 Legal Assessment II: General Principles of Administrative Law 192
11.7 Conclusions 195
References 195

11.1 Introduction

Electronic Child Records (ECRs) are currently being introduced and applied in youth care throughout the Netherlands. Prima facie, ECRs seem to be a mere digitisation of paper records, and hence, a logical step towards fulfilling the goals of effectiveness and efficiency pursued by e-government policy. A closer look into the developments in this area, however, reveals that ECRs will become a part of surveillance systems, through which the behavior of children and their social environment are continuously and closely monitored to generate data and profiles for public policy making. This trend can have an impact on children, care professionals, and their mutual relationship in various ways. Besides a possible shift to a

Contribution received in 2010.

S. van der Hof (✉)
TILT—Tilburg Institute for Law, Technology, and Society of Tilburg University, Tilburg, The Netherlands
e-mail: hof@tilburguniversity.edu

S. van der hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_11,

more effective youth care system with the objective of preventing victimisation of children and fostering their healthy and prosperous development throughout childhood; growing data intensity and disembodiment of relationships also amount to potential risks in light of new vulnerabilities, like system dependence or information security issues, and violation of fundamental values, such as personal freedom. Children have always had a special position within the law to foster their protection and welfare, but we may ask ourselves whether such laws still adequately address these new developments and, in particular, their potentially negative consequences.

This chapter aims to analyse the legitimacy of ECRs with regard to child welfare. It will attempt to answer the question as to whether in ECRs, the rights and interests of children are adequately safeguarded, measured against a human rights-based approach as well as the general principles of good governance.

It builds on research conducted by the author for the Netherlands Organization of Scientific Research on the construction of citizens' personal identities in new modes of government (van der Hof et al. 2010). Within this project, case studies were carried out, one of which addressed the development of ECRs. Through desk research and stakeholder interviews, these case studies analysed the construction of personal identities based on key concepts, in particular personal-data intensity, identification creep, abstracted identities, compound identities, invisible visibility. These concepts were identified in the conceptual and theoretical framework of the research. This chapter incorporates some of the findings of that research, but at the same time takes the subject a step further by particularly focusing on a human rights-based approach and general principles of good governance, and by exploring how ECRs can be assessed in view of both.

I will first set the stage by introducing three relevant social paradigms that form the backdrop against which the rest of the story will unfold, i.e., the informational society, the risk society, and the surveillance society. I will then proceed to describe relevant developments (Sect. 11.3) and potential impacts (Sect. 11.4) of ECRs. Section 11.5 assesses ECRs from a human rights-based perspective and Sect. 11.6 provides a legal assessment of ECRs by applying general principles of good governance. Section 11.6 finalises the chapter with conclusions.

11.2 Social Paradigms

ECRs are manifestations of modern society in which three social paradigms, i.e., informational society, risk society, and surveillance society, appear to converge. These scenarios are closely related, even mutually reinforced, and each immensely facilitated by ICTs. The focus of each of these phenomena is different though. The informational society generally has—despite the risks associated (for example, in areas of privacy and security)—a more positive connotation than the other two. The informational society holds opportunities for innovations that generate convenience and freedom, whereas the other two stem from negative premisses, like controlling potential risks and watching over individual behaviour to prevent

exigencies. The risk society and the surveillance society present opportunities for those who manage risks and are in charge of surveillance. From an individual's perspective, these societies are often qualified as lacking personal freedom, privacy, and transparency. Overall, social changes reflected here denote an apparent belief that we can engineer society through government policies so that social problems will disappear (termed 'maakbaarheid van de samenleving' in the Netherlands). Each of these scenarios will be briefly sketched in light of ECRs.

The informational society has fundamentally changed the social landscape and relationships in both the public and private sectors, including youth (health)care, by having 'information generation, processing and transmission, become the fundamental source of productivity and power' (Castells 1996, p. 21). Besides opportunities this also raises concerns. Society—including public administration—becomes a highly dynamic and increasingly complex environment, sometimes leading to modern Kafkaesque situations. Although digitisation of youth healthcare is merely a next logical step in modernising this policy area, the changes it entails will nonetheless have a profound qualitative impact on relationships and individual lives, as will be elaborated later on in this chapter. Moreover, digitised data are the raw materials on which both of the other scenarios thrive.

The move towards a risk society has already ensued for decades and typically tilts the serving and repressive government to a more calculating government (Beck 1994; Giddens 1998; Garland 2001). The idea is to reduce potential risks to acceptable risks by means of advanced rationalisation of decision-making processes. Consequently, a shift occurs from acting upon contingencies *ex post* to calculating the potentialities of future exigencies. Although it is early days yet, we see this scenario unfolding in the case of ECRs, given that, for example, the concept of high-risk youth and risk-management practices are gaining ground in youth care, both of which will be further explained in the next section.

Finally, the surveillance society also shows a perception of growing risk and interest to control risks, but in academic literature the emphasis is more on state monitoring policy and practices than modes of calculation (Lyon 2001, 2003). Surveillance is instrumental to risk-assessment, given that it produces the data that feed risk-evaluation processes through monitoring of online and offline behavior in society. Monitoring children and their social environment is one of the key objectives of ECRs in order to ensure their healthy development. ECRs are also much more sophisticated in achieving this goal than the good old paper records, by allowing for large-scale and systematic surveillance and, hence, creating elaborate pictures of children and their social environments.

11.3 From Simple Records to a Pervasive Monitoring System

The history of ECRs is a rather turbulent one. The original plan had been to develop a national ECR that would connect information systems with all youth healthcare organisations through one platform. However, public procurement

troubles resulted in a decentralised approach, in which municipalities chose and implement (and in some cases develop) their own ECR systems (van der Hof and Keymolen 2010). The local ECRs still have to comply with national specifications to allow for a more effective information exchange between youth healthcare organisations across the country. Thus it must be prevented that children—particularly those potentially at risk of experiencing psychosocial problems—can no longer be traced in the system when, for instance, they move to a new municipality. Ultimately ECRs will be connected to the nationally instigated Electronic Health Record to provide other healthcare professionals, like GPs, with access to medical data of children registered in youth healthcare.

In the Netherlands, children and adolescents from 0 to 19 years are periodically seen by youth healthcare professionals, such as child health centers ('consultatiebureau') or municipal health centers ('GGD' or 'GG&GD'), who monitor their physical, cognitive, and social development. All personal data on children was until recently kept in paper files. In 2010, these paper dossiers had to be replaced by ECRs. ECRs are based on the contents of the paper dossiers and contain information on the physical, cognitive, psycho-social development of individual children, their social environment (family, peers, education, etc.,) and with time, will also contain prenatal data. A standardised list of data, called 'Basic DataSet' ('BasisDataSet' or BDS), contains about 30 pages of data—potentially—collected by pediatricians and nurses during medial consultations at set times. Although the BDS is based on paper files, it has been supplemented with new data fields. Recently, personal profiles have been added to indicate the probabilities of children and adolescents who run psycho-social risks. Children who have a high-score on risk factors, like in the cases of divorced parents, poverty, aggressive behavior or depression, are labelled 'red' and are more closely monitored by youth healthcare professionals. Others are labelled either orange (medium risk) or yellow (low risk). These profiles also become part of the ECRs.

So far the developments regarding ECRs are confined to the youth healthcare, but we are still only halfway. The ECRs have become part of a snowball effect by raising the interest of other parties in extending their functionalities to other areas. Data pertaining to the social and emotional development of the child is potentially relevant for social services, schools, the justice system. Greater availability of such data might improve coordination within the youth care domain, and prevent abusive situations for children. Over the years, there have been profoundly sad and startling incidents involving small children, some being murdered within the realm of their own families. It is believed that better cooperation between youth care organisations could have prevented these incidents from happening.[1]

[1] The most well-known case is that of the three year old Savanna who was found dead in the back of her mother's and stepfather's car in September 2004. She had been systematically starved as punishment for naughty behaviour and was probably killed by choking on a piece of fabric while her mouth had been taped. Besides, convictions of both parents, the death of Savanna also led to criminal proceedings against the youth-care professional involved. Although the court decided she had been negligent in exercising her duties, she was not held criminally responsible

The ECRs are considered key to that objective, given that they are instrumental in achieving full integration of data on children and their social environment within youth care. Having a complete picture of every child is expected to provide an effective basis for timely warning and intervention in damaging and unsafe private situations. To that end, it is considered necessary for youth healthcare to be redesigned to incorporate ECRs into youth care records already established in the former context. Obviously, this raises issues concerning medical confidentiality and privacy. A broad-view on ECRs is, moreover, fueled by the concept of 'high-risk youths' ('risicojongeren'). These youngsters have to deal with a multitude of problems or serious arrears, both socially and individually and, they may be at risk of becoming school drop-outs, unemployed or even criminals. High-risk youths could be more effectively identified and dealt with, when cooperation between professionals is improved and monitoring or risk-indication mechanisms are in place.[2]

Whereas central government has until now, been reluctant to take such a broad-view, ECRs for youth care on a municipal level have acquired their own dynamics. The cities of Amsterdam, The Hague, Rotterdam and Utrecht are planning to connect, amongst others, social services, schools, youth care organizations, and mental healthcare organisations to the ECRs to better serve the child's interest. In their view, only a complete integration of all data available in each context will enable professionals to provide vigilant care to youngsters and to anticipate harmful conditions in their families and broaden social environment effectively. Rotterdam indeed aspires to introduce a duty for parents and caretakers to attend meetings with youth healthcare professionals to ensure that every child is registered.[3] These four large cities deal with significant exigencies concerning high-risk youths and have substantially invested in these broad ECRs, hence considerable economic interests are at stake as well.

[2] Alongside the ECRs, the Reference Index High-Risk Youngsters ('Verwijsindex Risicojongeren' or VIR) has been developed in order to identify and monitor risk factors amongst children and adolescents. The VIR collects risk reports (e.g., contacts with the police, drug or alcohol addiction, child abuse) concerning youngsters from various youth care professionals within and across municipalities and mutually informs these professionals on their involvement with these children in case of a 'match,' i.e., the system holds two or more reports on an individual child or adolescent. The VIR does not provide the professionals with actual information on the child, but merely provides a signal to all professionals involved. Nonetheless even mere risk signals may disclose information about the particular problems a child is dealing with, e.g., when he or she is reported by a medical specialist for addiction or eating disorder. See also Chap. 4 of this book.

[3] Currently, youth healthcare services are provided on a voluntary basis, although most parents are likely to respond to invitations to attend and have their children checked regularly. The obligation envisioned by Rotterdam is inspired by rules on compulsory school attendance and is intended to be endorsed by sanctions.

11.4 The Potential Impact of ECRs

ECRs efficaciously enhance information processing between youth healthcare organisations—and beyond—by allowing records to be transferred through a national information infrastructure. Consequently, children are more effectively 'embraced' by the system so that they cannot easily, disappear from the system completely. For organisations, ECRs signify reducing administrative effort, particularly when, in the future, they are connected to Electronic Health Records and allow for cross-healthcare referrals of patients. Moreover, they can support coordination of work processes of various professionals, hence, endorsing timely alerts of actual or potential exigencies and harm in respect of youngsters.

However, in a number of others ways these ECRs also have rather problematic elements which need to be considered. Digitisation of records in itself conveys qualitative changes to existing arrangements, because it accommodates almost effortless exchange of data between more parties than ever before.[4] Clearly it is a *conditio sine qua non* for the broad youth-care ECRs discussed previously. What is more, the implementation of ECRs enlarges data intensity, given that the potential number of data to be registered is extended and the purpose of broad youth-care ECRs is unmistakably to construct complete pictures of individual children and their social environment. Data intensity can easily turn into information overload and be as daunting to professionals as looking for the proverbial 'needle in the haystack.' Moreover, data intensity begs the question whether giving extra attention to high-risk youths is still an option, if the number of children identified by the system to be potentially at risk dramatically increases and disguises the actual cases deserving professional care and concern. More data does not necessarily result in more adequate care if it lacks relevancy or even quality and veils what is important.

Besides, ECRs are prone to function creep. Function creep signifies an incremental extension of a system's functions to other uses or contexts than those initially intended or specifically imparted in public policy. Accumulative steps, however small, they may seem, can eventually have a profound qualitative impact on those involved. From monitoring children through the intermittent registration of a growing amount of data, ECRs are gradually becoming part of sophisticated risk management practices in which children are categorised and labelled in light of more adequate youth care. In other words, registered data form the basis for probability calculations that determine the likeliness of individual children experiencing various kinds of developmental difficulties during childhood. Categorisation in itself is not unusual, given that public policy is often directed at particular groups, involving processes of both generalisation and reduction, often also called stereotyping (van der Hof and Leenes 2010). In youth care too, the primary focus

[4] In 2007, the Citizen Service Number ('Burger ServiceNummer'), was introduced; a unique personal identification number to be used in Dutch public administration (and to a certain extent beyond), which considerably facilitates the linking of data across public sector databases.

may switch from individual children to particular types of children when they are assigned certain risk levels, like the red, orange, and yellow categories mentioned previously. While care professionals still deal with individual children, their perceptions of children may nonetheless be framed by the attributed risk labels. What is more, such profiles or labels can take on 'a life of their own,' amounting to what may be called 'abstraction of personal identities,' i.e., a tendency of records or profiles constituting a 'reality' distinct from the one in which the individual lives (van der Hof et al. 2010). As long as these realities coincide there may not be a problem. However, if registered data are not adequately updated and, henceforth, incorrect at the end of the day, this may seriously affect professional decision-making processes and individual lives.[5]

A further danger of stereotyping is that it can lead to unjustified prejudice and discrimination. Van der Hof and Keymolen (2010) speak of 'stigmatised identities' to point at the danger of unwanted or unfair inclusion or exclusion of public services. It is paramount that in some way the authorities keep track of the actual person behind personal or risk profiles that are generated in these processes, so as to be able to adequately judge and decide on individual situations. Stigmatisation might more generally impact individual lives. It is difficult to give a prognosis of the long-term effects of stigmatisation on children and adolescents, but given the rather extensive legal retention period of 15 years for the data registered in the ECRs, individuals might be haunted by youthful lapses well into adulthood.

Moreover, the firm focus on risks is typical of modern society in which prevention, control, and safety are key (Garland 2001), as well as the belief that we can re-engineer social exigencies in a way that makes them disappear (Scientific Council for Government Policy 2008). In this socio-technological landscape, relationships are based on distrust rather than trust, which may negatively impact the relations between caregivers and children or parents. In relation to this, it is relevant to state that data will be made accessible to a larger audience of care professionals than before. Most policy documents are silent on how this correlates with medical confidentiality, and, more generally, it is likely that professionals may be reluctant to share sensitive data so as not to breach their relationship of trust with children and parents. Greater data intensity and interconnectivity can also propagate avoidance of professional care by parents or other caretakers. Some parents seem to refuse to fill in school doctor questionnaires, which seek amongst others, psycho-social data, because there is a lack of trust in ECRs and uncertainty as to what they entail for the future of their children.[6]

Finally, with the introduction of ECRs, technology fulfills a crucial role in youth (health)care. Accordingly, particular vulnerabilities, dependencies, and complexities enter this arena, which may impact the amount of trust that care

[5] The Dutch Ombudsman's 2009 Annual Report shows the tremendous difficulties that citizens are confronted with, if their data is incorrect or compromised and public administration does not take any responsibility for mistakes. One of the particularly complex areas is youth care, involving a mere 24 organisations in the VIR (*supra* n. 2).

[6] See NRC 2009.

professionals, parents, and youngsters have in the system. The ECRs contain highly sensitive data, which raises substantial concerns in light of information security. Additionally, technology may obtain a commanding effect by directing professionals towards predefined choices through default parameters, tick-off lists or other software routines, which can undermine professional autonomy or result in overlooking important factors not embedded in the system.

This section has particularly raised issues of critique in respect of ECRs. One may simply ward off these and other criticisms by declaring that if ECRs, however, small the percentage, better the lives of children who may otherwise come to harm, there is sufficient justification to put them in place. Undoubtedly, the necessity to provide children with safe environments in which they prosper and develop healthily is self-evident; however, this does not relieve public authorities from the obligation to carefully select, implement, and assess the measures taken for that purpose. The next two sections will address the legal environment in which the state operates when protecting children from harm and from the negative impact of monitoring practices. The starting point is that child welfare should always be at the forefront of the discussion.

11.5 Legal Assessment I: A Human Rights-Based Approach

It is paramount to assess any form of public policy in the light of human rights. Fundamental rights both stimulate and curtail the actions of the state towards its citizens, including children. In other words, fundamental rights promote human welfare and social reform but also confine state power. In this respect, children have a distinct legal status in that they are developing individuals and not (yet) fully autonomous. Children have rights and obligations under the law, but not in the same way as adults. Against this backdrop, the state has an important role in encouraging minors to develop their personalities and personal identity in a well-balanced manner, in order to become self-reliant and responsible adults.

Based on the universal rights of the child,[7] Willems (1999) speaks of the right of the child to become a person ('persoonswordingsdrecht'),[8] which can be further distinguished in the right of the child to become an optimal person and the right of the child to become a minimal person. The first refers to 'the right of the child to be brought up to optimal rationality, morality, and authenticity' (Willems 1999, p. 1002), more specifically including 'optimal development of one's personality/talents/abilities, optimal preparation for responsible life in a free society' (Willems 1999, p. 1005). The state should exert maximum efforts and resources to promote this right. The second right denotes the core right of the child entailing 'the whole

[7] As laid down in the UN Convention on the rights of the child, see http://www.unicef.org/crc/, accessed March 2010.

[8] With reference to De Ruyter 1995.

of socio-educational guarantees against child abuse, in the five variants of child physical abuse, child physical neglect, child emotional abuse, child emotional neglect, and child sexual abuse' (both citations Willems 1999, p. 1002). Here the state's role goes a step further, given that it has an obligation to ensure that 'each child under its jurisdiction becomes more than a minimal person' (Willems 1999, p. 1005). Generally, the state has a secondary educational responsibility in case of a lack of parental awareness, which might necessitate preventative measures (like parent education or juridical intervention) in light of child harm and abuse that, subsequently, should be balanced in order not to unnecessarily or even unlawfully intrude upon the privacy of parents and families.

Most importantly, Willems' stance is that the Netherlands is grossly negligent in addressing social abuse and harm of children in a structural, integrated, and preventative way. We might assume that since Willems made his statement, the situation in the Netherlands has not—significantly—improved, as evidenced by reports on child abuse and failures of adequate coordination within youth care. Moreover, quite recently the UN Committee on the Rights of the Child in its Third Periodic Report on the situation of children in party states expressed manifest concerns regarding the considerable extent of child abuse in the Netherlands as well as the inadequate procedures to detect and address child abuse (UN Committee 2009), which confirms that in fact the position of children is still precarious. The preventive measures Willems alludes to, in order to deal with the problems are socio-pedagogical and legislative in nature rather than technological, like ECRs. However, when talking of structural, integrated, and preventative measures, ECRs are exactly what nowadays may come to mind. Hence, how do ECRs fit in with the human rights-based approach with respect to children?

ECRs intend, amongst others, to provide risk indicators and risk alerts that allow professionals to take preventative action or at least intervene at an early stage when a child's optimal or minimal development is endangered. ECRs facilitate more efficient data exchange amongst care professionals and, henceforth, are instrumental to the modernisation of organisations. Enhancing the coordination of work between professionals through information systems can be useful and ultimately also children may benefit thereof, but a rights-based approach demands a careful consideration and balancing of child rights when designing and implementing new modes of operation. For all the good intentions of ECRs in terms of child welfare, the system may, nevertheless, have adverse repercussions on children's lives. It is not entirely clear what the long-term consequences of ECRs will be and how detrimental effects can be avoided or neutralised. Although face-to-face counseling between care professionals and children remains important, their relationship is increasingly influenced by ICTs. As we have previously seen, this may eventually fundamentally change their relationship. The sector increasingly comes to depend on technology, for instance the way in which data is presented, in channelling care professionals' actions, and in steering decision-making. The design of the system will have a tremendous impact on the relationships at hand and on individual lives of those involved. Willems' (1999) preventative measures would, for instance, be

directed at impeding stigmatisation of children by allowing for prevention of problems or at best timely intervention, whereas ECRs might precisely amount to that if children (or parents) are labelled inadequately by the system or if the system 'remembers' youthful lapses well into adulthood.

ECRs are also a strongly technology-driven solution for a great diversity of psycho-social and physical exigencies, and there are multiple goals—like preventing child abuse, identifying high-risk youths, identifying physical or socio-psychological disorders amongst individual children, supporting public policy-making—to be served by the system. In terms of the optimal and minimal development of children, ECRs offer both options or at least do not make a distinction between either of them. To be sure, both constitute essential public tasks, but each has its distinct features and approaches. The question arises whether ECRs are the most effective answer to the problems in the youth care context for each of the purposes implied. For instance, when it comes to identifying children in need of care and protection, we might ask ourselves whether pervasive monitoring of all children is necessary. It seems likely that—most of—these children are already known to professionals and that the system should, therefore, focus on more adequately coordinating actions among these professionals, as the VIR mentioned earlier is designed to do.

Key to discussing the ECRs is how these systems promote the best interest of the child to grow up in a safe environment with ample opportunities to develop its personality and talents. Besides the protection of societal interests, child welfare is an important consideration in establishing modern surveillance systems, like ECRs, however, to what extent and how the rights and interests of children (and their families) are incorporated and protected in the system is completely unclear, because seldom are they made explicit in policy documents and the design of the system. The next section will further draw upon this conclusion from the perspective of the general principles of good governance.

11.6 Legal Assessment II: General Principles of Administrative Law

A second angle contended here concerns the general principles of proper administration ('algemene beginselen van behoorlijk bestuur'), which include the principles of the prohibition of détournement de pouvoir (i.e., using a competence for other reasons than legitimate purposes), reasonableness, legal certainty, trust, equality, proportionality, principle of due care, and motivation (Addink 1999). These principles demarcate public action and the informational society has left their applicability untouched. Dutch administrative courts have a long history of applying these principles in the context of judicial review.

More generally, Prins (2007) states that the use of technology in citizen–government relationships demands special attention for these principles in various ways and the points she makes are relevant for the ECRs too. First, the principles

of due care demand that the government meticulously informs citizens in order to enable them to protect their interests and rights adequately, which may signify that practical and institutional arrangements have to be adapted to new situations in ways that prevent or mitigate negative consequences and risks for citizens. Although, ECRs are implemented for the benefit of children, we have seen earlier that these systems have drawbacks, including information security risks, raised complexity of decision-making processes, non-transparent mistakes in decision-making, inadequate data quality, and stigmatisation, which can adversely affect their lives. At best, public authorities need to assess the—potential—impact of innovations on public administration and individual citizens carefully and make amends where things take a wrong turn. In a more desirable scenario, various options for designing and using the ECRs would be carefully balanced in view of fundamental values and rights. An example is the VIR that aims at coordination and cooperation between professionals when action concerning an individual child is necessary. It does so, however, without by definition, sacrificing confidentiality and privacy in the design of the system, because it merely reports that a professional is involved with a youngster but does not provide data on the nature of the involvement. However, even in the VIR these different kinds of information cannot be separated completely, since having a medical practitioner in drug addiction or eating disorder report the child, clearly tells other VIR participants involved, something about the child's problems.

Moreover, it appears that the speed of installing ECRs in youth care is appreciated more than diligence. In this respect the overarching principle of legality, which informs the administrative law principles, is relevant in light of ECRs.[9] This principle requires public policy to have a foundation in formal law. Remarkably, the sole specific legal basis for ECRs is a mere stipulation in Article 5 of the Act on Public Health ('Wet Publieke Gezondheid,' Stb. 2008, 461) obliging youth healthcare to digitalize record-keeping of patient (i.e., child) data.[10] It seems that legal preconditions for the development of ECRs, and more particularly their extension to areas for which they were not initially intended, are tenuous, which raises questions of legitimacy, legal protection, and legal certainty. In addition, the principle of proportionality can be held to require public authorities conscientiously to consider the extent of particular measures in terms of accessibility, functionalities, and goals, and comprehensively to motivate why all-inclusive (in terms of data subjects and professional users), pervasive monitoring and risk-management systems are necessary in youth care.

Furthermore, Prins (2007) points out that the principles of sound administration require public authorities systematically and consistently to give account of the effects and benefits of the implementation of technologies for the state, individual

[9] This principle is not one of the general principles of sound administration but constitutes the foundation of our 'rechtsstaat' (rule of law). It is not codified in the Dutch Constitution. Rather its applicability to relations of citizens with the state is presumed (Voermans and van Bijsterveld 2000).

[10] ECRs are, thus, governed only by generic legislation, like the Personal Data Protection Act.

citizens and society as a whole in light of fundamental principles of the rule of law ('rechtsstaat'). Such a rights based approach contrasts with instances in which the state solely refers to general policy objectives, like improving the efficiency of service delivery or the effectiveness of law enforcement. There seems to be a tendency in which the state puts utility before a rights-based approach in which child rights are expressly taken as a starting point for policymaking and carefully balanced in the design of information systems. In the case of ECRs, child welfare is high on the list of policy objectives, for very good reasons we might add. As was mentioned earlier, however, the state must explain much more thoroughly and exactly how ECRs are to the benefit of children and parents, and what rights they have in respect of them. Moreover, these rights and the conditions for use should be well-defined by law focusing specifically on the development of ECRs. This is an obligation the state has taken on when becoming a party to international conventions, like the UN Convention on the Rights of the Child and the European Convention on Human Rights. Fundamentally, an approach that defies general principles of sound administration can, therefore, challenge human rights and invoke further scrutiny by the European Court of Human Rights or the UN Committee on the Rights of the Child.

According to Prins (2007), transparency of the government should become the default position in citizen–state relationships, which means, amongst others, that 'black box' technology must be opened up by public authorities. This would also support accountability of public policy. Indeed, the growing complexity of society, in good part as a result of technological developments, makes the principle of transparency as one of the principles of sound administration more and more central. Even though transparency is already sheltered by personal data protection legislation, as well as the obligation of the state to observe openness ('openbaarheid'), citizens could benefit from a more direct reference to transparency in the process of innovating public administration and the subsequent operation of modernised decision-making processes. We may safely assume that ECRs will not make a public-sector context that is already quite complex, less complicated and, therefore, it is essential to provide transparency of decision-making processing and of how to hold government accountable for mistakes. Transparency of ICT mediated decision-making processes can be coupled by giving parents and children not only more insight into decision-making processes, but also giving them control over the management and use of their data in ECRs.

Finally, the principle of equality must be observed when treating children differently. Obviously, the aim of ECRs is to do just that by singling out the children who are at risk in some way or another and provide them with the care and protection they need. We can easily agree that such differentiated regimens should be perfectly accepted in terms of justice and fairness. However, this may be different in cases of unfair inclusion or exclusion of care and protection. Such cases may, for example, occur when associated real-life and system realities start diverging, because data sets or profiles are not up to date or simply wrong. Decidedly, both the principles of equality and due care would be at stake here.

11.7 Conclusions

This chapter has analysed developments concerning the digitisation of youth (health) care, more particularly the introduction and potential impact of ECRs, and assessed these systems in light of a human rights-based approach and the general principles of sound administration. Such an assessment is important and timely because ECRs have taken on a dynamic of their own in the youth care domain, and seem to have developed into pervasive monitoring tools capturing the lives of our children in a very detailed manner; predicting their futures in sophisticated ways. The outcome of this development may impinge heavily on the natural course of children's lives, if they turn out to be youngsters at risk. Care and protection of children, and adolescents should unmistakably be at the forefront of youth care work, and ECRs can be important in making the sector more efficient and effective in preventing children from being harmed and encouraging a positive development for those at risk. At the same time, we should not throw the baby out with the bathwater by establishing a system that, rather than helping the child or parent, may adversely impact their lives.

Respecting human rights and the general principles of sound administration, the state should have an eye for child rights and show due care in designing a system that may deeply affect human lives. Merely stating that ECRs are in the interest of child welfare is not enough. Child rights must become part of the system by ensuring that it does not produce stigmatizing effects and by safeguarding children's freedom to develop themselves, even if it means making mistakes. Furthermore, the state has special obligations under the rule of law as well as international conventions, to ensure that ECRs comply with existing values and rules, and are founded on an adequate legal basis. ECRs should be designed and used in an efficacious and transparent way. All in all, policy-makers and system designers still have a long journey ahead of them.

References

Addink GH (1999) Algemene beginselen van behoorlijk bestuur [General Principles of Proper Administration]. Kluwer, Deventer

Beck U (1994) The reinvention of politics, towards a theory of reflexive modernization. In: Beck U, Giddens A, Lash S (eds) Reflexive modernization. Polity Press, Cambridge

Castells M (1996) The rise of the network society. Blackwell Publishers, Oxford

De Ruyter DJ (1995) Het recht om persoon te worden: een criterium voor het opleggen van pedagogische hulp. In: De Ruyter DJ, De Ruyter PA (eds) Opvoedingshulp geboden; Pedagogische criteria voor het opleggen van hulp, theoretisch en praktisch bezien. Utrecht

Garland D (2001) The culture of control, crime and social Order in contemporary society. Oxford University Press, Oxford

Giddens A (1998) Risk society, the context of british politics. In: Franklin J (ed) The politics of risk society. Cambridge, Polity Press, pp 23–34

van der Hof S, Keymolen E (2010) Shaping minors with major shifts, electronic child records in the Netherlands. Information polity (forthcoming)

van der Hof S, Leenes RE (2010) Gedeelde en samengestelde identiteiten in de publieke dienstverlening [Shared and compound identities in public service delivery]. Research Commissioned by Alliantie Vitaal Bestuur, The Hague, Tilburg University

van der Hof S, Leenes RE, Fennell S (2010) Framing citizen's identities, the construction of personal identities in new modes of government in the Netherlands. Research Commissioned by the Netherlands Organisation for Scientific Research, Tilburg University, p 266

Lyon D (2001) Surveillance society, monitoring everyday life. Open University Press, Issues in Society Series, Buckingham

Lyon D (2003) Surveillance as social sorting, privacy, risk and digital discrimination. Routledge, London

National Ombudsman (2009) De burger in de ketens [The Citizen in Chains]. Verslag van de Nationale Ombudsman over 2008. http://www.ombudsman.nl/ombudsman/jaarverslag/2008/no-jvs-samenvatting-2008.pdf

NRC (2009) Code rood als voorspeller van opvoedingsproblemen. NRC Handelsblad, 4 March 2009

Prins JEJ (2007) Technocratie en de toekomstagenda van de Nationale ombudsman [Technocracy and the agenda for the future of the national Ombudsman]. In: Werken aan behoorlijkheid. Boom Juridische Uitgevers, Den Haag

Scientific council for government policy (2008) Onzekere veiligheid [Uncertain security]. Wetenschappelijke Raad voor het Regeringsbeleid, The Hague, October 2008

UN Committee (2009) UN Committee on the rights of the child, consideration of reports submitted by states parties under Article 44 of the Convention. Concluding observations, Netherlands, 27 March 2009. http://www2.ohchr.org/english/bodies/crc/docs/co/CRC-C-NLD-CO3.pdf

Voermans WJM, van Bijsterveld SC (2000) Inleiding hoofdstukken 5 en 6: wetgeving, bestuur en rechtspraak. In: Koekoek AK (ed) De Grondwet. WEJ Tjeenk Willink, Deventer, pp 388–400

Willems JCM (1999) Wie zal de Opvoeders Opvoeden? Kindermishandeling en het Recht van het Kind op Persoonswording [Who will Educate the Educators? Child Abuse and the Right of the Child to Become a Person] (with a summary in English). TMC Asser Press, The Hague

Chapter 12
Legitimacy Issues Regarding Citizen Surveillance: The Case of ANPR Technology in Dutch Policing

Charlotte van Ooijen

We need to change course before it is too late.
Board of Chief Commissioners 2005, p. 4.

Abbreviations

ANPR Automatic Number Plate Recognition
RFID Radio Frequency Identification

Contents

12.1 Introduction 198
12.1.1 Nodal Orientation as a New Police Strategy 198
12.1.2 Legitimacy Problems as a Reason and a Result 199

Contribution received in 2010.

An earlier version of this chapter was presented to the Study Group on Information and Communications Technologies in Public Administration at the 2009 Annual Conference of the European Group on Public Administration (EGPA), 2–5 September 2009, St Julian's, Malta.

C. van Ooijen (✉)
TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands
e-mail: C.W.vanOoijen@tilburguniversity.edu

C. van Ooijen
Tilburg School of Politics and Public Administration, Tilburg University, Tilburg, The Netherlands

S. van der hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_12,

12.1.3 Chapter Outline 201
12.2 Legitimacy: Indicators, Relevance and Dilemmas for Nodal Policing 201
12.2.1 Assessing Legitimacy 201
12.2.2 Relevance to Nodal Policing 203
12.2.3 Legitimacy Dilemmas 203
12.3 Research Methods 206
12.3.1 Position of the Researcher 207
12.3.2 Informants 207
12.3.3 Observation 208
12.3.4 Interviews 208
12.3.5 Document Study 209
12.4 The Power of ANPR 209
12.4.1 Technological Power 209
12.4.2 The Nodalville ANPR System 210
12.4.3 ANPR Applications 211
12.5 Legitimacy Issues in ANPR Policy-Making 212
12.5.1 Legality 212
12.5.2 Moral Justification 213
12.5.3 Social Acceptance 214
12.6 Final Remarks 215
References 215

12.1 Introduction

12.1.1 Nodal Orientation as a New Police Strategy

In 2005, the Board of Chief Commissioners of the Dutch police (in the rest of this chapter referred to as 'The Board') published a new vision memorandum on policing. This report entitled 'The Police in Evolution'[1] portrayed a reorientation of the task and position of the police. The presented mission, vision, and strategy were not supposed 'to do more—or less—than offer a course for developments to follow with a view to tailoring police tasks as closely as possible to society's requirements' (Board of Chief Commissioners 2005).

'Nodal orientation' was highlighted as a key concept in the new police strategy. Derived from the work of Manuel Castells (2000) on the network society, the police distinguished a space of flows alongside a space of places, urging them to take up a new strategy concentrating on the nodes and flows constituting the space of flows. In their own words: 'the nodal orientation ("infrastructure policing") leads to surveillance of the infrastructure, or rather, the flows of people, goods, money, and information that use the infrastructure to move from one place to another' (Castells 2000). In order to realize this surveillance of flows, the police needed to develop information-driven working methods and secure the exchange of information with partners in the safety domain (Board of Chief Commissioners 2005). This emphasis on the importance of information encompassed a more

[1] In Dutch: 'Politie in Ontwikkeling.'

technology-intensive way of working, which explicitly included the use of 'catch scan technology where observations and registrations of people and vehicles are compared with a wide range of databases (e.g., unpaid fines, stolen vehicles, missing number plates, known suspects)' (Board of Chief Commissioners 2005). In subsequent policy documents, this technology is predominantly called Automatic Number Plate Recognition (ANPR) and will as such be referred to in this chapter. ANPR is a complex system of cameras, networks, databases, and software programs which is used by the police to obtain valuable police information from traffic data. By means of 'smart' fixed or mobile cameras, number plates of passing vehicles are digitally gathered to be linked to numerous types of police information. Consequently, the police are able to survey their regional infrastructure for (suspected) burglars, drunk drivers, drug runners,and other offenders of the law.

The concept of nodal orientation has been a heavily debated topic in both academic and police circles. Recently, Bekkers and van Sluis (2009a) provided an overview of the current state of affairs regarding nodal orientation. In their contribution the authors set out the core characteristics of the concept, explain its strategic implications and examine the followed implementation strategy. They state that the implementation of nodal orientation in police practice can be characterized as 'island innovation,' a collection of so far unconnected projects. They conclude by shedding some light on the future of nodal orientation and provide some advice for the rehabilitation of what they consider to be a beautiful concept.

12.1.2 Legitimacy Problems as a Reason and a Result

In a review of the contribution by Bekkers and van Sluis (2009a), Bruggeman (2009) expresses three matters of concern which all point to legitimacy problems regarding nodal orientation. First, he questions how far the police may and should go concerning the 'random' application of nodal orientation, especially in the light of privacy issues. Second, Bruggeman wonders whether the current manner in which nodal orientation is used has any future at all when looking at ongoing technological developments. He argues that technological possibilities, such as the connection of Radio Frequency Identification (RFID) to the Internet, calls for a different approach than the current one. Consequently, he casts doubt on whether further investments in nodal orientation can be legitimated. The third issue raised is a need for self-regulation by the police to uphold the democratic quality of nodal policing. In conclusion, Bruggeman states that once these three issues have been addressed, this will stimulate a more lasting acceptance among citizens. Summarizing Bruggeman's concerns, he identifies legitimacy problems in terms of legality, justification, and social acceptance. In the subsequent reply by Bekkers and van Sluis (2009b) they affirm the importance of citizens' privacy as well as the issue of democratic accountability of nodal policing. In addition,

they emphasize that nodal orientation is not merely a matter of technology, but has political relevance as well and as such needs political-democratic legitimation.

This is a remarkable state of affairs when reassessing the reasons as to why a new vision and operational concept were needed in the first place. As I will argue further in Sect. 12.2, part of the reasons which led the police to develop the strategy of nodal orientation can be understood as possible threats to organizational legitimacy. An indicator for this assessment can be found in a quote from the introductory chapter of the report 'Police in Evolution.'

> There is a feeling that the police should perform better. Wherever the expectations and performance levels are difficult to reconcile, citizens become dissatisfied, they lose confidence in the police and the police lose their legitimacy. The police aim to continuously optimize their performance and, at the same time, their public image. Part of this process involves the profession forming a shared, coherent view on what will contribute to promoting safety. The present document contains the guiding principles of such a view, expressed as a mission, a vision, and a strategy for the coming years (Board of Chief Commissioners 2005, p. 21).

Apparently, according to the police, the potential loss of legitimacy could be countered by developing a new strategy. The respective contributions by Bekkers and van Sluis, and Bruggeman, however, reveal that the strategy of nodal orientation seems to pose some legitimacy risks of its own.

How can nodal orientation enforce the legitimacy of the police and at the same time cause legitimacy problems? How can this tension be understood? In this chapter I aim to take the discussion between Bekkers and van Sluis, and Bruggeman further by identifying legitimacy dilemmas in the practice of nodal policing. What do police actors consider to be legitimacy issues when dealing with nodal orientation? How do they interpret and address these issues? Answers to these questions may help to assess what the police are already doing to overcome legitimacy problems regarding nodal orientation, as well as what issues may be found troublesome. The empirical arena I studied concerns one of the 25 regional Dutch police forces, which I will refer to as 'Nodalville.' In the Nodalville police region, ANPR technology has played an important role in the implementation of nodal orientation. I conducted this case study between December 2008 and April 2009.

Legitimacy-related questions about the nodally oriented application of ANPR could be: 'does catching a handful of criminals justify the 24/7 scanning of all vehicles passing a particular ANPR-camera?,' 'Which information should be allowed to be connected to the registered number plates?' or 'Why should innocent citizens' data remain stored in police databases?' Legal theory and moral philosophy could be helpful to answer these kinds of questions. In this case study, however, I have taken a different approach towards legitimacy issues. Instead of asking these kind of normative questions myself, I am interested to see whether these questions are posed by the actors involved in ANPR policy-making, and how these are addressed. In other words, how important is legitimacy in police practice and how do police actors deal with it?

Consequently, the central research question for this chapter is:

What are legitimacy dilemmas in police policy-making concerning the nodally oriented application of ANPR and how are they dealt with?

12.1.3 Chapter Outline

In order to understand the legitimacy dilemmas in the case study, the concept of legitimacy is first explored in literature. Theoretically, it is important to determine what the concept entails, what its different aspects are and why it is of relevance to the issue of nodal policing. The literature review results in a theoretical overview of legitimacy dilemmas and operational indicators of legitimacy issues. In the third section, I describe the research methods of this case study, which can be characterized as qualitative–interpretive. Fourth, I will describe the context and use of ANPR in the Nodalville police region. In the fifth section, I will discuss what legitimacy issues arise in ANPR policy-making, what legitimacy dilemmas these pose and what actions police actors take in reaction to the issues at hand. Finally, I present the conclusions and reflect on the importance of legitimacy in policing practice.

12.2 Legitimacy: Indicators, Relevance and Dilemmas for Nodal Policing

12.2.1 Assessing Legitimacy

Legitimacy is an abstract concept which is not easy to handle (Zouridis 2009). Yet it is handled in the practice of public administration. Sometimes this happens literally, for example, by mentioning it in a policy report. The 'Police in Evolution' report shows 24 instances of the word 'legitimacy' in 18 pages. This quantitative measure indicates that the issue of legitimacy is of some relevance to the Dutch police, which is not surprising when looking at Beetham's argument that all power structures seek legitimation (Beetham 1991).[2] This, however, does not help to form a thorough understanding of the meaning of legitimacy for policing. In order to gain such an understanding, we must turn to academic literature about legitimacy to find operational measures which can help to recognize legitimacy issues in public administration.

Gaining, having, and maintaining organizational legitimacy is far from an easy task to realize. According to most theorists, legitimacy concerns the need to fulfill

[2] Cited in Sparks et al. 1996, p. 85; Zouridis 2009, p. 293.

criteria which are about the right with which a public organization wields power (Vedder 2007a, p. 6). This 'right to rule' (Simmons 1979)[3] is of a multi-dimensional nature, encompassing legal, morally normative and social aspects (Vedder 2007a, p. 7). These three dimensions, which can be referred to in terms of legality, moral justification, and social acceptance, make up a general structure through which the legitimacy of any given power structure can be expressed and evaluated (Beetham 1991).[4] In the following, I briefly discuss these three dimensions, after which I will discuss possible reasons for the police to pay attention to legitimacy issues concerning nodal orientation (Sect. 12.2.2). Finally, I highlight some complicating factors and dilemmas involved in the assessment of an organization's legitimacy (Sect. 12.2.3).

12.2.1.1 Legality

In a democratic society such as the Netherlands the power of the state is founded in law. Legality can be described as the principle that government may command and forbid citizens to do things, under the condition that the law allows it, and in a way which is in conformity with legal rules and principles of justice (Michiels 2006). This aspect of legitimacy, thus refers to the conformity to rules. It may appear to be easily testable by, for example, checking whether a certain action is in accordance with the law. Problems arise when it turns out that either there is no regulation about a specific action or there is a just a broad rule which requires a great deal of interpretation to make it applicable to the specific situation. Empirical indicators for legality as legitimacy are references to rules, regulations, and procedures.

12.2.1.2 Moral Justification

This aspect concerns justification in relation to moral norms and values. Even though this is the only one of three aspects which can contain substantive criteria (values and norms with specific content), such as respect for human rights, it is not restricted to these alone. Procedural criteria such as accountability and responsibility may also be relevant (Vedder 2007a).

12.2.1.3 Social Acceptance

This aspect entails the consent or representation of those involved or affected. Zouridis (2009) identifies three indicators for social acceptation. These are:

[3] Cited in Copp 1999, p. 5.

[4] Cited in Sparks et al. 1996, p. 85.

support, trust, and obedience/compliance. In addition, Vedder (2007b) points out that this matter is not solely restricted to citizens' acceptance, but can also take shape by consulting powerful or knowledgeable organizations. To what extent the police manifest a concern for these matters forms an indicator for the practical relevance of this legitimacy dimension.

12.2.2 Relevance to Nodal Policing

From two points of view, it can be argued that the issue of legitimacy is of relevance to the police. From a moral point of view, public organizations ought to strive for legitimacy. It would be amoral to exercise power without legitimation by established rules, shared values, and social acceptance. From a practical point of view, public organizations need to strive for legitimacy in order to survive. Vedder (2007b, p. 198) calls this striving for legitimacy 'for reasons of political efficiency and effectiveness.'

Legitimacy is a measure for the quality of public administration and, therefore, an important guiding principle (Hendriks 2007). It sets boundaries and obligations to the policies and actions of public authorities, thereby safeguarding citizens' fundamental rights. At the same time, it is a complex principle, because of the different meanings and possible interpretations in the practice of public administration causing difficulties for public officials in their decision-making. The issue of legitimacy is especially relevant in situations where the public organization interacting with citizens is very powerful (Zouridis 2007). A powerful organization can become even more powerful once it has incorporated information technologies in its policies and practices (Zuurmond 1994), thereby making the issue of legitimacy even more important. ANPR constitutes such a technology.

From a theoretical perspective, there are two reasons why the legitimacy of the police cannot be taken for granted, and therefore, should be reconsidered.

The police signal a decreasing effectiveness in their task of safeguarding society and fighting crime, because of several changes in society. The police themselves realize that 'efficiency and efficacy are now important pillars for the legitimacy of policing' (Board of Chief Commissioners 2005). The changes in society also refer to the social acceptance of the police, as indicated in Sect. 12.1.2. The technology-intensive strategy of nodal orientation implies an increase of police power, which needs legitimation.

12.2.3 Legitimacy Dilemmas

In striving for legitimacy, the police may encounter a number of dilemmas which have to do with the complexity of the idea of legitimacy. A dilemma involves making a tough choice. Before elaborating on the different kinds of

dilemmas, I first explain why the adherent choices are this difficult. Reasons can be found in the variability of the three dimensions (legality, moral justification, and social acceptance), the idealistic nature of legitimacy and the legitimacy scale.

12.2.3.1 Variability

Legitimacy is an ideal which an organization should always try to reach from a moral point of view. What is unfortunate for the practical fulfillment of this striving is that legitimacy itself cannot be defined in absolute terms. The idea of what is legitimate changes over time along with societal and legal developments. The police may now be considered legitimate in manifesting themselves as a key player in the safety domain, because it is their legal task to fight crime, and society expects the police to do so. The morally normative idea that crime is an undesirable matter for our society and should, therefore, be banned is the foundation of the legal and social support for the police task. Apart from the fact that the notion of what is considered to be a crime can change over time, ideas on how to protect society from it can also alter. The police themselves signal that media, politics, and citizens have become more dominant in the safety domain (Board of Chief Commissioners 2005). Beetham (1991) contends that the specific content of legitimating principles and beliefs is to a great extent historically and culturally variable.[5] Therefore, what legitimated a Dutch police force in the 1970s may not rightfully justify the actions of this police force in 2009. This variability of evaluative criteria very much complicates the assessment of an organization's legitimacy. Would it, for example, be legitimate for an organization to anticipate on future events to legitimize their actions? This matter makes it even more interesting to see what the police consider to be indicators for their legitimacy.

12.2.3.2 The Idea(l) of Legitimacy

One could pose the question whether an organization needs to completely fulfill (if at all possible) the requirements of all legitimacy dimensions in order to be legitimate. From an empirical point of view the question would be whether the police indeed tries to do so and finds all dimensions to be equally important. According to Zouridis (2007, 2009), legitimacy concerns 'a power configuration being simultaneously legal and authoritative, and its justification' (Zouridis 2007, p. 97, respectively, Zouridis 2009, p. 295), indicating that an organization would have to fulfill all requirements. From Beetham's (1991) scheme[6] we can

[5] Cited in Sparks et al. 1996, p. 85.

[6] Cited in Sparks et al. 1996, p. 85.

infer that a certain degree of illegitimacy is unavoidable. The scheme shows a form of non-legitimate power for each dimension. He distinguishes illegitimacy (breach of rules), a legitimacy deficit (discrepancy between rules and supporting shared beliefs or an absence of shared beliefs), and delegitimation (withdrawal of consent). All three forms of non-legitimate power are a realistic option, which an organization should try to prevent from happening. In doing so, the morally normative dimension is logically primordial to both the regulatory and the social dimension of legitimacy, because the last two may be instrumental to fulfilling the first (Vedder 2007a). This point is also made by Copp (1999, p. 3) when he highlights the issue of moral authority as being crucial for legitimacy.

12.2.3.3 Legitimacy Scale

The concept of legitimacy so far has been discussed in reference to public organizations in its entirety. For the discussion on legitimacy issues regarding nodal policing, it is relevant to make a distinction between occurrent legitimacy on the one hand and dispositional legitimacy on the other. The latter refers to the legitimacy of an organization in its entirety, whereas the first involves the legitimacy of a particular activity (Vedder 2007a). These two scales may be at odds with each other because a legitimate organization (whose exercise of power is legitimized by legal rules, moral values, and social acceptance) can perform non-legitimate actions. Such an organization may, for example, make a policy decision which is not socially supported. On the other hand, there may be a non-legitimate organization performing legitimate actions.

12.2.3.4 Dilemmas: Contradictions Between Dimensions

Legitimacy dilemmas can arise when a particular action or organization is found legitimate from the point of view of one dimension and illegitimate from another. Then, the issue is to determine the weight of the respective dimensions. If we were to theorize about concrete legitimacy dilemmas concerning nodally oriented ANPR, the following scheme could be drawn. The scheme describes hypothetical situations which are based on technical, legal, and organizational possibilities, and not on actual applications (Table 12.1).

These are theoretical legitimacy dilemmas. We do not yet know whether police actors actually experience these dilemmas while implementing nodal orientation and how they deal with them when considering the complicating factors of variability, ideal legitimacy and scale. To what extent can these dilemmas be identified in policy-making concerning ANPR for nodal orientation? How important are legality issues in the policy-making process? How do police managers justify the use of ANPR technology? Are relevant stakeholders consulted and for what reasons?

Table 1 Examples of theoretical legitimacy dilemmas concerning nodal orientation

	Occurrent (action)	Dispositional (organization)
Legal–moral	Even if the law would not allow it (yet), the police might be inclined to gather and store ANPR data on all important nodes in the region because they would consider it to be necessary to catch offenders	The police could decide to operate within the limits of the law, while at the same time feeling morally obliged to go beyond these (in order to be effective in fighting crime)
Social–moral	The police could feel morally obliged to use ANPR to catch the modern criminal, while stakeholders might not embrace the technology (yet)	Other stakeholders in the safety domain could demand that the police make it their primary concern to protect citizens rather than use all available means to fight criminals, whereas the latter activity might be of greater value to the police
Legal–social	Violation of citizens' privacy rights by gathering and saving ANPR data might be granted under strict legal conditions, whereas surveys could show that people found this completely unacceptable	The police could decide to operate within the limits of the law, but feel pressured by other stakeholders in the safety domain to do more

12.3 Research Methods

This study can be characterized as an endeavor to understand how police actors involved in ANPR policy-making perceive and handle this technology, making this an interpretive–qualitative research. In this study, policy-making is considered to be a non-linear process in which formal decision-making at the managerial level and work floor decisions at the implementation level influence each other. In reaction to the top-down approach of policy-making, this can be called a bottom-up approach in which policy implementation is viewed as part of the policy-making process rather than a separate process.[7] Therefore, both formal decision-making and operational experiences with ANPR are included in this case study. This methodological choice is not merely theory-driven, but has an empirical foundation as well. As worded by one of the police chiefs I interviewed, 'The police are very much an organization of "do-ers." At times, they perhaps insufficiently think things through. But they do manage to stimulate a whole lot with the thinkers by letting things happen in practice.'

When dealing with ANPR, whether this happens in daily police business or in writing policy documents, police actors make sense of this particular technology in a particular context and a particular situation. Their perception of what ANPR is and what it can do for policing is crucial to the policies being formed. This process of sense-making by police actors can be called the first hermeneutic in this research. The second hermeneutic consists of me as a researcher trying to make

[7] See also Hill 2009, pp. 202–204.

sense of this process. I seek to understand how police actors deal with legitimacy dilemmas concerning ANPR. As a consequence, there is a double hermeneutic in this research. Because of the double hermeneutic, I speak of 'data generating' instead of 'data gathering,' since the research data in this case study are constructed within this particular context, rather than laying there to be found by the researcher.[8]

Findings in this chapter are based on the study of one Dutch police force. Data generating methods included participatory observation, interviews, and document study.

12.3.1 Position of the Researcher

As a researcher I was a visible observer in the police organization. I was granted official access and received an access card to police buildings, an e-mail account, a user name and password for the computer network and had a physical work space. I could walk in and out whenever I wished. This access was granted because the police are very interested in legitimacy issues concerning the application of ANPR. I promised to address this issue and write a report especially for the police force. My presence might have triggered informants to act more consciously than they normally would have. In order to prevent informants from feeling exposed or perhaps even compromised and to stimulate them to speak and act freely, I promised anonymity to the individual actors as well as to the police force as a whole. Therefore, in this chapter I have not linked quotes to specific job functions or used names and speak of 'the Nodalville police force.' Three key informants, who served as my formal contact persons within the organization, played an essential role in the data generating process.

12.3.2 Informants

I distinguish three key informants from other informants in this case study because my contacts with them were more extensive than with others and they regularly pointed me to new sources of information for my research. Using a network metaphor, I would say these three people were the nodes in my network of informants, documents, and events.

Two of the three key informants worked as policy advisors in the department responsible for all policy development concerning information technologies. My desk was situated in their office, enabling me to overhear phone calls, listen to their conversations with colleagues, and engage in them as well. Moreover, they

[8] See also Yanow 2007, pp. 109–121.

actively informed me about policy developments taking place during the days I was not physically present. My other key informant led a division responsible for all ANPR data management. All requests for ANPR data from within and outside the police force were dealt with by this 'ANPR-division.' Therefore, this key informant was able to provide me with adequate information about the practice of ANPR.

Other informants included people from within this particular police force and six people who are actors in the ANPR policy process, but are not actually part of this police force. The latter group consists of actors who are either members of the national ANPR program office or the local district attorney's office. I found the informants through the method of 'snow-balling,' which is based on asking each informant I met whether they could recommend another person I could talk to. I started this process with my key informants and proceeded until I felt I was not learning anything substantially new for my research, The 'snow-ball' also stopped sometimes when people did not respond to my request to meet. Information generated from and with the informants proceeded through interviews and participatory observation. Additionally, I conducted a document study.

12.3.3 Observation

Between December 2008 and April 2009 I spent several working days at the office to shadow my two key informants.[9] For practical reasons I planned these days around most of the interviews I wanted to conduct. On these days I was able to engage in day-to-day conversations with the people working on the floor, which gave me a good idea of what the ongoing policy topics regarding ANPR were. I made field notes of every conversation I had and discussions I overheard. In addition to these office days my third key informant invited me to the ANPR-division for a couple of days enabling me to have a look at the data software. He took me through some query options and answered more detailed questions about how the data system works and its application. Furthermore, I made two visits to one of the key ANPR data gathering locations. I was able to see the camera positions, traffic flows and secret camera van where data was entered in the software system.

12.3.4 Interviews

Besides carrying out these spontaneous, yet sometimes lengthy, conversation style interviews which I mentioned earlier, I also conducted semi-structured interviews

[9] On the method of shadowing see also Geuijen et al.f 2007, p. 132.

with 12 informants. A total of seven interviews were conducted with informants representing the Nodalville police force. The other five informants were either national police representatives or employees of the local district attorney's office. The local police informants were mainly asked to describe their involvement with ANPR and elaborate on successes and problems they encountered. The other informants were asked to provide information about the policy context in which the local police force operated and comment on their experiences with the local police force. The interview protocol relied on open-ended questions, leaving room for additional questions tailored to the specific interview situation.

12.3.5 Document Study

I studied documents such as policy chapters, work instructions and internal (memos, intranet postings, e-mails) and external correspondence (newsletters, publications, and presentations) to see whether and how legitimacy issues are addressed.

12.4 The Power of ANPR

12.4.1 Technological Power

The power of the concept of nodal orientation is that it offers a strategic perspective by reframing existing practices and projects, and framing new practices (Bekkers and van Sluis 2009b). This is precisely what has happened in the police region of Nodalville. They had started using ANPR shortly before the 'Police in Evolution' report appeared and ideas about nodal orientation could descend to the Dutch police forces. This police force has been using ANPR for law enforcement purposes since 2004 but is gradually expanding the range of applications to innovative ways of crime fighting. At the same time, the number of ANPR cameras owned by the Nodalville police has substantially increased, resulting in more data gathering. Using ANPR at infrastructural nodes does not automatically imply a strategic repositioning of the police. van Bruul et al. (2008) argue that in most cases this is no more than a technical approach to traditional police work.[10] Even if this were the case in Nodalville, ANPR is still a very powerful tool.

In this section, I will discuss the power of ANPR technology in the police region of Nodalville, as this is an important aspect of discussion on legitimacy. A core characteristic which makes ANPR a powerful technology is that it combines location data with personal data enabling the police to monitor citizens'

[10] Cited in Bekkers and van Sluis 2009a, p. 52.

every move faster and more accurately, than ever before. The police use of ANPR can, therefore, be understood within the context of other initiatives in public administration to use location-based services (LBS) in public policy.[11] The specific power of ANPR becomes apparent when considering the amount and nature of the data being gathered, the way in which this data is managed and some actual applications in police work. The objective of this account is to provide some general insights, which are necessary to understand the discussion on legitimacy issues in Sect. 12.5 of this chapter. Therefore, it is not a complete or entirely detailed description of ANPR applications in Nodalville.

12.4.2 The Nodalville ANPR System

ANPR involves more than just a camera taking pictures of number plates. It is a complex system which can convert traffic data into valuable police information. I put an emphasis on 'can,' because, as will be demonstrated, not all data actually amounts to information.

Technologically speaking, the Nodalville ANPR system consists of cameras for data gathering, databases for data storage, a network connection for data access, and software for data linkage and analysis. I will briefly highlight some basic aspects of each of these technological components. The Nodalville police force owns both fixed and mobile cameras. The fixed cameras cover the major entry and exit roads and gather data for 24 h a day, 7 days a week. The mobile cameras in police vehicles are switched on more irregularly. What data do these fixed and mobile cameras exactly gather? A camera automatically takes pictures of the number plates of all passing vehicles. The underlying software then converts these digital photos into alphanumerical data. Both the picture files and the alphanumerical number plate data are stored along with data on location and time. The network connection then enables an authorized police officer at the office to access this data within seconds. On average, more than 80,000 data registrations are made per day from one fixed location. From one fixed location alone on an average over 80,000 passages are registered per day. At the time of writing, all data is stored for 4 months and permanently deleted afterwards, except for the data which in the meantime has been selected for further police investigation. A software program helps the police to enrich the millions of stored ANPR data records in order to obtain information which can be of value in different kinds of police processes. The program creates hitlists of number plates with which 'something's up,' to use the words of a police informant. At this point in time, the police define the criteria for inclusion on a hitlist by looking at the car owner's past or present offenses. Examples range from unpaid speeding fines, alcohol-related offenses and drug

[11] See also van Ooijen and Nouwt 2009.

trafficking to wanted felons. By linking police data on offenses to data on car owners, hitlists of attention-worthy number plates are generated.

12.4.3 ANPR Applications

Basically, the hitlists can be used in two types of applications, either direct pursuit on the one hand, and further investigation on the other.

12.4.3.1 Direct Pursuit

Direct pursuit involves comparing number plates to a previously composed hitlist in real-time to take immediate action. The Nodalville police organize special action nights to actually remove the 'hits' from the anonymous traffic flow. On these occasions, police motor-cyclists are present at one of the fixed camera locations. Upon a signal from their colleague who is watching the ANPR system, they drive up to a particular car and escort it to the side of the road where police officers are awaiting to deal with the particular offense. This, for example, involves collecting fines, checking alcohol abuse or making an immediate arrest. Passing cars which are not registered on any hitlist, the so-called 'non-hits,' remain in the ANPR system because of their possible relevance for the second type of application.

12.4.3.2 Further Investigation

The reasoning of the Nodalville police is that all ANPR data, both 'hits' and 'non-hits,' may prove to be of use later on for crime fighting purposes. Specific queries help the police to have the necessary information emerge from the huge amount of stored data. For example, the police have used the ANPR system to retrospectively track the movements of a murder suspect. A police investigator explains how ANPR was used in the particular case:

> We gave a presentation in the court of law, in which we showed a virtual overview of a map. We used little light bulbs to show our observations of the historical data, ANPR and camera footage. That way we could, so to speak, let them drive towards the scene of the crime. Well, that made quite an impact, also in the court of law. That is the beauty of it … That is the power of combining your data … So far, I have not had a single question about the acceptability of this data to the court of law. We simply explained in the official report how we got it, how it is made available and this is simply accepted. No questions. None at all. No.

The quote above could be interpreted as an indication that the use of data gathered by means of ANPR would not pose any legitimacy problems. The informant also states that policemen working with this technology do not consider

this to be an issue. One could wonder whether the fact that neither the court of law nor the involved police investigators consider this particular application to be illegitimate means that there are no legitimacy issues concerning ANPR or that Nodalville police officers do not pose any legitimacy-related questions at all.

Another way of using ANPR data for further investigation is the analysis of movement patterns of a particular group of people. The Nodalville police have compiled a hitlist of home burglars. On this list there are names and number plates of people who are known to have been convicted, suspected or otherwise involved in burglaries. This list is updated weekly and used to find suspects of particular burglaries and enable the police to catch burglars red-handed. Finding suspects is done by geographically plotting committed burglaries and hitlist movements. Also, the time of the burglaries and the time at which the fixed camera locations were passed by are taken into account when determining which cars could be connected to which burglaries. At the same time, the system allows for exclusion of particular suspects. Furthermore, movement patterns are analyzed to determine at what time a burglar returning home is likely to pass by one of the camera locations. This allows the police to position a field officer at the scene so they can single this person out of the traffic stream, possibly finding the stolen goods in the trunk of the car.

12.5 Legitimacy Issues in ANPR Policy-Making

Analysis of the interviews, field notes, and documents reveal that the Nodalville police force is concerned with legitimacy issues regarding legality, moral justification, and social acceptance. However, not all dimensions receive equal attention in ANPR policy-making.

12.5.1 Legality

The way in which the Nodalville police deal with legality issues can be characterized as:

12.5.1.1 Consciousness of the Need for Legal Legitimation

Currently, there is no law in the Netherlands which clearly determines how the police may or may not use ANPR. Nodalville policy makers actively investigate which laws are applicable and come to the conclusion that the current legal framework does not provide sufficient guidance on what course of action should be followed. This assessment, however, does not pose a reason to not develop a course of action at all.

12.5.1.2 Instrumental Legality

In order to overcome this legal insecurity, the police have developed an instrumental concept of legality. They do not wait for legal security to arrive by itself, but actively engage in political discussions in order to help create legal possibilities. As one informant formulates it: 'We want to prevent having a suspect in front of a judge who then considers the ANPR data to be an illegitimate evidence.'

12.5.1.3 Legality as a Risk

At the same time, policy documents show that legality issues are considered to be a risk as well. The police express their concern that the development of legal norms and political discussion may put a stop to the originally designed and enacted plans. This is especially the case for possible violations of citizens' rights to privacy.

Legality is thus considered an important criterion for the legitimacy concerning ANPR, but not a criterion which is completely beyond the power of the police.

12.5.2 Moral Justification

The Nodalville police are not particularly concerned about this legitimacy dimension, which is remarkable, since it would be logical to turn to morally normative arguments, considering there is a lack of legal guidance. How then do the Nodalville police justify ANPR?

12.5.2.1 Effectiveness and Efficiency

For most actors it is quite clear that ANPR already increases the effectiveness and efficiency of the police force and will do so even more in the future, in the face of expanding applications. Informants and documents usually refer to success stories of the direct pursuit application in law enforcement to support their claim, and use this argument to legitimize further applications of ANPR. We see that the legitimacy of a particular police action (the direct pursuit application) is used to refer to the legitimacy of the police organization as a whole. 'Policing becomes more effective,' is something I have heard more than once. In addition, this claimed dispositional legitimacy is used to justify yet another police action (the further investigation application). As a result, the provided justification is not a sound one.

12.5.2.2 Nodal Orientation

The concept of nodal orientation is also often used as a means of justification. 'ANPR is efficient, it is effective, and of course it is nodal orientation.' Most

informants state this without properly explaining what nodal orientation entails and why this is of importance.

12.5.2.3 Frontrunner Position

Another often expressed argument is that the Nodalville police force is the frontrunner as far as ANPR is concerned. The image and position of the Nodalville police as an innovation-minded police force among the other forces is apparently an important consideration in ANPR policy-making.

12.5.3 Social Acceptance

The police pay attention to issues of social acceptance in various ways.

12.5.3.1 Remaining Informed

Policy makers actively follow the ongoing political and societal discussion on ANPR. For this purpose, they consult research reports, follow the news media and consult online forums where citizens express their opinions on the matter.

12.5.3.2 Strategic Consideration

The police themselves assess the importance of certain stakeholders. Policy makers state that they take what some actors have to say more seriously than others. Nonetheless, they also listen to actors they find to be 'less relevant,' but more for the sake of listening, than for the actual outcome. The Dutch data protection authority, for example, did receive a formal reply from the Nodalville police on one of their reports, but was granted little importance in the actual policy-making process. This strategic consideration, however, can strengthen the police's apparent consideration of the social dimension of legitimacy.

12.5.3.3 Cautious Communication

The Nodalville police limit society's awareness about ANPR through their conservative communications policy. There have been press releases about the direct pursuit application, but these do not give away details about the technology. They merely mention the results of a particular action. On certain occasions some information about crime fighting applications is provided, but only in very general terms and upon a journalist's request.

12.5.3.4 Influencing Social Acceptance

Even though this police force has representatives in all national discussion boards on ANPR, this does not automatically mean that the social dimension of legitimacy is honored in the strict sense of the word. Informants expressed their intention to participate in these groups, mainly to educate other police forces on how they should handle ANPR and to influence the discussion on legal norms. 'We now discuss these matters in order to prevent being stopped later on.'

12.6 Final Remarks

The variability of legitimacy, resulting in uncertainty regarding legality and social acceptance of ANPR is dealt, with in two ways. On the one hand, the police strive to actively influence both dimensions. On the other hand, the police rely on moral justification in terms of effectiveness and efficiency while not substantially supporting these claims. In order to increase legitimacy, the police need to find substantial support for this moral claim. The fact that the police are partly aware of this problem is a good start.

This case study shows that policy makers are very sensitive towards legitimacy issues, but mainly for pragmatic reasons. The chances of fulfilling ANPR's potential are increased by legitimizing actions, such as researching legal boundaries and talking to policy stakeholders.

This case study has an ironic twist if we look back at the initial debate concerning the legitimacy of nodal orientation. In the 'Police in Evolution' report, securing citizens' privacy was cornered as an argument for the implementation of nodal orientation. Reasons for this were that nodal orientation was supposed to be less invasive to citizens and not randomly applicable. In this case study, however, privacy only emerges as a complicating matter; an argument against ANPR. Perhaps further support can be found for these substantive values so that they can provide a new impulse for the discussion on the legitimacy of nodally oriented ANPR.

References

Beetham D (1991) The legitimation of power. Basingstoke, Macmillan

Bekkers V, van Sluis A (2009a) Nodale politie in Nederland. Een Tussenstand Van Zaken [Nodal police in the Netherlands. An intermediate state of affairs]. Panopticon 30:49–54

Bekkers V, van Sluis A (2009b) Reactie Op De Nabeschouwing van Prof. Dr. Willy Bruggeman [Reaction to the review by Prof. Willy Bruggeman]. Panopticon 30:55–56

Board of Chief Commissioners (2005) Police in evolution. Vision on policing. Board of Chief Commissioners/NPI, the Hague

Bruggeman W (2009) Nabeschouwing Bij De Tekst 'Nodale Oriëntatie' [Review of the text 'nodal orientation']. Panopticon 30:54–55

Castells M (2000) The rise of the network society. Blackwell, Oxford
Copp D (1999) The idea of a legitimate state. Philos Public Aff 28:3–45
Geuijen K et al (2007) Dutch Eurocrats at work: getting things done in Europe. In: Rhodes RAW et al (eds) Observing government elites: up close and personal. Basingstoke, Palgrave Macmillan, pp 131–159
Hendriks F (2007) Legitimiteit Van Bestuur: Moeilijkheden En Mogelijkheden Van Gezaghebbend Machthebben [Legitimacy of administration: difficulties and possibilities of exercising power with authority]. In: Cornelissen EMH et al (eds) Betoverend Bestuur: Legitimiteit, Vitaliteit, Meervoudigheid. Den Haag, Lemma, pp 63–74
Hill M (2009) The public policy process. Harlow, Pearson Longman
Michiels FCMA (2006) Hoofdzaken Van Het Bestuursrecht (Main tasks of administrative law). Kluwer, Deventer
Ooijen CW, van Nouwt J (2009) Power and privacy: the use of lbs in dutch public administration. In: van Loenen B et al (eds) SDI Convergence, research, emerging trends, and critical assessment. NCG, Delft, pp 75–88
Simmons AJ (1979) Moral principles and political obligations. Princeton University Press, Princeton
Sparks RF et al (1996) Prisons and the problem of order. Clarendon Press, Oxford
van Bruul I et al (2008) Leiderschap Als Knooppunt. Een Studie Naar De Rol Van Leiderschap in De Diffusie Van Nodale Oriëntatie Binnen De Nederlandse Politie. School voor politieleiderschap, Warnsveld
Vedder A (2007a) Questioning the legitimacy of non-governmental organizations. In: Vedder A (ed) NGO involvement in international governance and policy: sources of legitimacy. Leiden, Nijhoff, pp 1–20
Vedder A (2007b) Towards a defensible conceptualization of the legitimacy of NGOs. In: Vedder A (ed) NGO involvement in international governance and policy: sources of legitimacy. Nijhoff, Leiden, pp 197–212
Yanow S (2007) Interpretation in policy analysis: on methods and practice. Crit Policy Anal 1:109–121
Zouridis S (2007) De Legitimiteit Van Recht En Bestuur: Signalen Voor Legitimiteitserosie Geanalyseerd [The legitimacy of law and administration: analysing signals of eroding legitimacy]. In: Cornelissen EMH et al (eds) Betoverend Bestuur: Legitimiteit, Vitaliteit, Meervoudigheid. Den Haag, Lemma, pp 93–116
Zouridis S (2009) De Dynamiek Van Bestuur En Recht: Over De Rechtsstaat Als Bestuurswetenschappelijk Fenomeen [The dynamics of administration and law: about the constitutional state as a phenomenon in the study of public administration]. Den Haag, Lemma
Zuurmond A (1994) De Infocratie: Een Theoretische En Empirische Heroriëntatie Op Weber's Ideaaltype in Het Informatietijdperk [The infocracy: a theoretical and empirical reorientation on Weber's idealtype in the information era]. Den Haag, Phaedrus

Chapter 13
The Introduction of Biometrics in The Netherlands: An Evaluation Under Data Protection and Administrative Law

Annemarie Sprokkereef

Abbreviations

ICT	Information and Communication Technology
RFID	Radio Frequency Identification
DPA	Data Protection Act

Contents

13.1 Introduction 218
13.2 'Classic' and 'Second Generation' Biometrics 218
13.3 Biometric Applications in the Private and the Public Domain 219
13.4 Some Observations on Unintentional Side Effects of Dutch Government Policy on Biometrics 222
13.5 A Data Protection Approach 223
13.6 An Administrative Law Approach 225
13.7 Conclusion 227
References 228

Contribution received in 2010.

A. Sprokkereef (✉)
TILT–Tilburg Institute for Law Technology and Society, Tilburg University, Tilburg, The Netherlands
e-mail: a.c.j.sprokkereef@tilburguniversity.edu

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_13,

13.1 Introduction

Principles of proper administration form the basis of legitimate and due government. These include the prohibition to use a public competence for non legitimate purposes, and the principles of due care, reasonability, legal certainty, trust, proportionality, and motivation. This chapter explores current developments in the use of biometrics in the Netherlands in the wider context of the shift towards eGovernment. New forms of information handling in eGovernment are of course, also bound by the above principles. This raises some questions which need to be answered. Does eGovernment pose new challenges to the value of principles of proper administration in practice? Are the principles of proper administration rigorously applied to the introduction of biometric data in government information systems? With these questions in mind, I will give a short overview of the current use of biometric technologies and assess their impact on the evolving information structure of Dutch eGovernment.

When using the term 'biometrics,' I refer to automated decisions identifying or authenticating individuals using information technology and 'classic' biometric data: unique body data such as finger scans and face scans. The use of 'classic' biometrics has received attention in current social science literature predominantly from the risk society and the surveillance society perspectives. Both risk management and surveillance policies have come to heavily rely on the facilitating abilities of ICTs and the powerful informational infrastructure ICTs help to create. The integration of 'classic' biometric data into ICT infrastructures has introduced some social and legal issues that will be discussed below. I will however, first briefly explain which technological developments make an assessment of the impact, of the use of new types of biometrics in information systems even more complex in the future.

13.2 'Classic' and 'Second Generation' Biometrics

Towards the end of the 1990s, biometric technologies started producing many innovative applications with enhanced features which were enabled by advanced scanner and ICT technologies. Together, these technologies created new possibilities for large-scale identification processes through the use of face, finger and iris scans, large databases, and the linking of different sets of data. Data on the individual human body thus became useful information that could be integrated into an information infrastructure. There are a range of 'classic' biometric applications already in use in the private and the public domain and these will be discussed below.

One of the more recent developments in the field of biometrics is the shift towards embedded ICT systems in a physical environment. Radio Frequency IDentification (RFID), and sensor, nano or wireless technologies increasingly

allow communication between objects. Innovative ICT technologies and ambient intelligence systems enable the creation of embedded systems for digital monitoring and identification of individuals in public places. These systems can use a range of body characteristics that are not unique to one particular person. Examples of such body data are facial expressions, pulse, body temperature, and sweat levels that can vary in a person depending on the particular situation at hand. I will label these data 'situational' biometric data. 'Soft' biometric data are another group of data that can be used by public or private authorities in a wide range of (automated or non-automated) decisions on people for identification, authentication, monitoring, assessing or profiling processes. These 'soft' biometrics (age, weight, gender or ethnicity for example) cannot be used to uniquely identify a person, but can be used to assist in identification or, for example, profiling, when several different biometrics are combined. The implications of the use of these second generation biometrics will not be addressed here as these systems are not yet in operation in the Netherlands. It should be clear however, that the new generation of biometrics will pose new questions about the way this information is handled in future (Mordini and Tzovaras 2010).[1]

13.3 Biometric Applications in the Private and the Public Domain

In order to provide a context for this chapter, it is useful to first determine the pervasiveness of biometric applications in the Netherlands.

Article 27 of the Dutch Data Protection Act requires the Dutch Data Protection Agency ('College Bescherming Persoonsgegevens') to keep a register of all projects that have to be notified under data protection law. A notification requirement ('meldingsplicht') applies to all forms of automatic data processing, with the exception of processing falling within the exemption decree ('vrijstellingbesluit'). However, as the register does not specify whether the processed data are biometric, its value is only limited in the quantification of the use of biometrics. Existing inventories regarding the use of biometrics in the public or the private domain are still relatively incomplete (De Hert and Sprokkereef 2009b). Yet, despite the lack of reliable information, it is undisputed that the number of applications using biometrics in the private sector has considerably increased.[2] Improved measurement methods and reliability rates, decreased physical sizes of sensors and accompanying price reductions have all played a part in this process. Biometric applications have also been integrated into other products, such as cars and computers, and companies selling biometrics have employed marketing strategies designed to create a market (De Hert and Sprokkereef 2009a, p. 24).

[1] See also Chap. 3 of this book.

[2] See the Netherlands Biometrics Forum's Position paper at http://www.biometrieforum.nl

In 2008, Dutch schools first started using biometrics as an access key for staff and parents to enter the school premises. Originally, these schools never intended acquiring a biometric entry system, and indeed never paid for it: they were offered free trials to use the system (De Hert and Sprokkereef 2009a, pp. 24–26). This approach was based on the idea that supply would lead to the creation of a demand ('markufacturing') for biometric systems and this would be followed by a rapid growth in the number of private or semi-public institutions using biometric applications.

There are already a number of bigger projects in operation. The semi-public and established Privium scheme at Schiphol airport has more than 25,000 members. A biometric access system used by a university in Amsterdam has more than 20,000 users and there are more systems in use. The commercial applications used in the private sector cover mostly convenience applications: hand scan applications for access to semi-private institutions, such as sport clubs, finger scan systems used by video shops, disco bars, coffee shops, etc. However, a pilot project for supermarkets enabling payment using a finger scan was discontinued.[3]

Some applications serve safety objectives. Examples are finger scan systems that help enforce bans on access to swimming pools to visitors who have a history of misbehavior, or car rental companies who use this system to ensure the safe and timely return of their vehicles.

Users of a private biometric system often do not know how their data is handled and stored. Details concerning enrollment, storage and deletion of data at all these locations are sketchy,[4] and the likelihood of those private systems being linked to public ones is unclear. Indeed, in the case of the swimming pool some evidence of public-private sharing of data has been found (De Hert and Sprokkereef 2009a, b).

The three main government biometric initiatives are the introduction of electronic identity documents with biometrics, identification processes using biometrics within the criminal justice system (CIS 2008), and use of biometrics in registration and identification of foreigners and visitors. Of these examples, only the use of biometrics for identification purposes in the criminal justice system is not a direct reflection of EU developments. All the other government applications that are being introduced have been initiated, or at least re-enforced, by decisions made at EU level (De Hert 2007).[5]

Dutch passport or identity card holders are issued a machine readable document with an embedded RFID chip for storing a face scan and two finger scans.[6] An amendment to the Passport Act has also enabled the storage of these biometric data in a central database. Article 4b(4) of the amendment to the Passport Act provides that public prosecutors can request access to data in the database, under the strict

[3] The pilot received national media coverage: Dutch television news item: http://nos.nl/artikel/72986-klanten-ah-betalen-met-vinger.html

[4] Observations by experts contributing to an open discussion as reported in the Knopjes report.

[5] See also Chap. 14 of this book.

[6] See also Chap. 23 of this book.

rules applying to access to data in the context of a criminal investigation. Since September 2009, when applying for a passport, all Dutch citizens are required to provide their local town halls with their fingerprints.[7] The obligatory nature of the provision of biometrics crosses previous boundaries concerning the concept of ownership of the body. It does constitute a claim of the State to rights of access to a citizens' body because, if a citizen refuses to provide their bodily characteristics, they will not be able to travel abroad, claim health insurance, vote in the elections, etc. For the efficient use of biometrics in travel documents a further reader infrastructure needs to be in put place. The full infrastructure for this (including facilities at border check points) is expected to be ready by 2011.

Since the mid-1990s, finger scans of foreigners (including other EU citizens)[8] are included in the foreigner database, for the purpose of identification. The finger scans are stored to prevent identity fraud, especially look-alike-fraud, and to facilitate the efficient implementation of the Foreigners Act 2000. The finger scans are not stored for law enforcement purposes.[9] Such use of biometrics that is targeted at a socially and economically vulnerable group as foreigners is of concern for democratic, humanitarian, and legal reasons and deserves more attention than it has received to date (Dijstelbloem and Meijer 2009, p. 253). The Ministry of Foreign Affairs has also finalized an infrastructure for enrolling the biometric data of visitors to the Netherlands in a VISA administration system.

A law on identification in the criminal justice system, based on the use of biometric finger scans, was adopted in July 2009. Its goal is to bring about reliable identification of suspects and convicts. The Act on the Identification of Suspects, Convicts, and Witnesses ('Wet identiteitsvaststelling verdachten, veroordeelden en getuigen')[10] recognizes four ways of identifying a person: a declaration, presentation of a valid identification document, a face scan, and finger scans. The law indicates which type of identification is required or allowed at which moment in time, and also introduces new elements such as the suspect having to identify him or herself before a court. The necessary infrastructure is expected to be completed by 2011.

These systems are not optional, so that control of individuals over their biometric data has been dramatically reduced. Conversely, possibilities of State authorities being able to compare an individual's data sets have considerably increased which is likely to result in changes in existing balances of power.[11] The Meijers Committee, for example, has pointed out that the Act on Compulsory Identification ('Wet op de identificatieplicht') creates a situation where suspects' finger scans in police files will be automatically compared with finger scans stored

[7] In February 2009, the student A. Boudewijn started a court case claiming the right to object to inclusion of his fingerprints in the central database: http://www.nu.nl/binnenland/2185458/student-rechter-privacy-paspoort.html

[8] See Art. 1, e, m of the Foreigners Act.

[9] However, see Chap. 14 of this book.

[10] Staatsblad 317 (28 July 2009).

[11] For a more detailed analysis see the report: especially Chap. 4.

in the above-mentioned foreigner database. The Committee concluded that this is contrary to national and international law, citing in support of the ECJ *Huber* case[12] and the ECHR *Marper* case.[13] The Committee stated that the necessity of using these data for criminal law purposes was not sufficiently demonstrated. Thus, the resulting increased risk of stigmatization of foreigners was not proportional to the benefits of the law.[14]

Apart from these existing government applications, new, smaller, and larger government biometric information systems are in preparation or already in place. These concern amongst others, access control for civil servants to government buildings and access control in jails. There are also plans for the inclusion of biometrics on chips in driving licenses.

13.4 Some Observations on Unintentional Side Effects of Dutch Government Policy on Biometrics

It is widely accepted that there is no comprehensive vision behind the introduction of biometrics in the Netherlands (Grijpink 2009). In the absence of such a clear policy framework, applications have tended to be introduced ad hoc per policy domain rather than across domains, often as a follow up of agreements at the European level. Coordination and coherence between different sectors is minimal, which is partly a result of the fact that the Ministries of Justice, Internal Affairs and Kingdom Relations, and Foreign Affairs initially each pursued their own policies, and only recently started to coordinate these efforts (Knopjes 2009).

As the implementation of biometric applications is highly complex, knowledge and expertise within one government department is rarely sufficient to implement an application. Proper implementation presupposes an assessment of the overall impact of the biometric application on processes, procedures and existing balances of power. As extensive cross-domain coordination and continuous policy readjustment has been lacking, there are considerable gaps in knowledge and impact assessment in the public sector. The Dutch Biometrics Forum has called for detailed measures for bringing about complaint and fall back procedures, preventive measures against biometric identity theft, including the foundation of a national centre for the protection of biometric data, and concrete measures such as compensation for damages, etc.[15]

---

[12] *Huber* v. *Germany*, European Court of Justice, Case C-524/06, Judgement of 16 December 2008.

[13] *Marper* v. *United Kingdom*, EHRM 4 December 2008, Appl. Nos. 30562/04 and 30566/04. See further Chap. 14.

[14] Letter of the Meijers Commission, CM0901, 22 January 2009.

[15] In its position paper available at: http://www.biometrieforum.nl/tiki-list_file_gallery.php?galleryId=15

Consequently, when private parties started to implement applications for their own purposes, they lacked a clear reference framework to assess the proportionality, safety, and privacy consequences of these applications. No government guidelines have been issued so far. Efficiency and security arguments have persuaded citizens to accept innovative biometric applications, and in this process, civil rights interests have tended to be overlooked. On several occasions, the Dutch Data Protection Commissioner has been urging public and private institutions to strengthen the information provision on their data handling practices, and to take steps to protect the longer term rights of users.

A 1999 report already concluded that designers, developers, suppliers, and users of products using biometrics for identification, authentication, or exposure of emotions needed to consider ways to protect the privacy of users. The report recommended the following measures to minimize or eliminate privacy risks: different criteria for the use of identification and authentication, decentralization of storage and encryption, decentralized storage of templates and the verification process, use of different encryption keys and algorithms to encrypt the personal data (including biometrical data) in different databases. The original biometrics should preferably be destroyed after the derivation of the digital template (Hes 1999, p. 63). The safety of biometric data, once collected, is not very well documented. It is not known to what extent the private sector adheres to the ground rules as laid down by this report and in, for example, the position paper of the Dutch Biometrics Forum (2009). Traditional inspectors who visit sites to enforce compliance with specific laws are often not equipped to check electronic documents, biometric or computer applications, and databases (Knopjes 2009, p. 68).

So what are the principles that should safeguard the rights of the users of biometric applications? I will first look at data protection law and then at administrative law.

13.5 A Data Protection Approach

The existing legislative framework concerning data protection applies to the use of biometrics. No separate legislation on handling biometric data has been proposed or adopted. In general, Dutch data protection regulations create a legal framework for the lawful the processing of personal data. Data protection legislation thus aims at making existing processing practices transparent, but does not prohibit them as a rule. Accordingly, individual ownership of personal data is not recognized, but individual controlling rights are granted instead. Governed by the 'enabling logic' of data protection, the law has not been an obstacle for the diffusion of biometric technologies.

Although the Data Protection Act (DPA) does not contain specific provisions that explicitly refer to biometric data, there has been hardly any discussion about the conditions under which biometric data should be considered personal data. Sending a notification of use to the DPA is all that is required to start a new

biometric application. Normally, the DPA does not take further steps after it receives the notification of the processing of biometric data. Formally, the notification to the data protection authority does not imply a 'go.' On the contrary, the notification allows the authority to react if this is needed. In practice, and due to staff constraints, this rarely happens. As it is not necessary for the processor or controller to wait for a 'green light,' the controller can start the processing straight after notification. In practice, the role of the data protection authority therefore has been reduced to receiving notifications, making an administrative check on them, and registering notifications that are accessible through its website. The DPA has been asked thrice to issue a preliminary opinion on biometrics. The first is the opinion relating to an access control system for a disco bar with a biometric pass. The second is the DPA opinion on the amendment to the Passport Act in order to introduce biometrics in 2001, and again in 2007.[16] The third is a 2003 opinion on the use of face recognition and other forms of biometrics for access control to public events, combined with their use for police investigations.[17]

In the first opinion, the DPA concluded it was inevitable that use is made of templates of the face (containing information about race) for the identification of troublemakers. The DPA also stated that the use of personal data for marketing purposes should not include biometric data, and that the processing to this end should be separate from other purposes. The DPA concluded its opinion with several recommendations, including conditions for storage and security (encryption of templates and membership card numbers), and for the operation of the biometric system. The DPA also requested that any systems already installed would have to comply with these requirements.

In 2001, the Dutch Minister of Internal Affairs and Kingdom Relations requested the DPA's advice on new paragraphs proposed to Article 3 of the Passport Act.[18] On examination of the provisions, the DPA first pointed out that the new Passport Act would allow biometric data to be stored by the appropriate authorities. The DPA then proceeded to conclude that it did not find sufficient arguments to support the necessity of such a measure. It also stated that even if there were such a necessity, the Passport Act would still need to be based on the 'purpose limitation principle,' whilst in the current wording, the purpose was open ended. In a second advice of 30 March 2007, this argument was repeated, and the DPA argued against (de-)central storage, warning for the effect of 'function creep.'[19]

The third, and most concrete, DPA opinion on the legal requirements to be fulfilled when introducing a biometric system is an answer to a request for an

[16] CBP, Wijziging Paspoortwet z2001-1368 (invoering biometrie), 16 October 2001.

[17] CBP, Vragen over de inzet gezichtsherkenning z2003-1529, 3 February 2004.

[18] CBP, Wijziging Paspoortwet z2001-1368 (invoering biometrie), 16 October 2001.

[19] CBP, Wijziging Paspoortwet advies z2007-00010 (invoering biometrie), 30 March 2007, 5, http://www.cbpweb.nl

opinion on the protection of personal data and the use of face recognition technology.[20] The system concerned involved the use of a smart card that served as an entry ticket to large-scale events. The smart card contained an identification number, a limited period of validity and a face scan (digital template) of the holder. In this case, there was a strong link between access control and identification. As the templates were stored in an event database, the use of the smart card was not restricted to access control. Therefore, the objectives of the access control system needed careful examination, especially when visitors have no other option than to use the system. The DPA concluded that when violation detection only depended to a limited extent on the templates stored in the event database, then the use of such a system tended to be disproportional. If the use of the system does not produce benefits compared to existing instruments for detecting violations, then the concept contains unnecessary processing of data. Through this opinion, the DPA confirmed that unnecessary processing of data is illegal.[21] The third DPA opinion thus introduced the basic condition of proportionality in respect of increasing safety by using of face recognition technology.

The Dutch Data Protection Authority's advice is not binding. In practice, the opinions of the DPA carry little weight. For example, the Passport Act was passed without further discussion of the DPA 2007 opinion in Parliament. Biometrics hardly feature in debates on data protection law. The First Phase Evaluation of the Data Protection Act report, is an obstacle analysis of the implementation and application of the DPA (Zwenne et al. 2007). It is noteworthy that there is no DPA case law on biometrics yet. This 211 page report does not mention biometrics even once. The final conclusion of the report is that many rights that arise from the DPA are not effectively exercised through a lack of familiarity with these rights (Zwenne 2007, p. 211). Thus, in conclusion, one of the core objectives of the DPA: to increase the transparency of data processing though the granting of rights and obligations and the introduction of a regulatory authority, has not been fully achieved. This conclusion coincides with the observation previously mentioned regarding non-transparent private and long-term civil rights interests of users of biometric applications. In practice, data protection law is therefore unable to act as a protector of the rights of users of biometric applications.

13.6 An Administrative Law Approach

Principles of proper administration form the basis of legitimate and due administration. These include the prohibition to use public authority for non legitimate purposes, and the principles of due care, reasonability, legal certainty, trust,

[20] CBP Face recognition technology, z2003-1529, of 3 February 2004, http://www.cbpweb.nl/downloads_uit/z2003-1529.pdf?refer=true&theme=green

[21] See the full opinion on a detailed test of the concept of data processing: CBP 27 May 2004, z2003-1529.

proportionality, and motivation. Prins (2007) has applied these principles to the use of technology in citizen–state relationships, and convincingly argued that in this case they place a heavy responsibility on public authorities. In this section, I will engage in a similar exercise as regards the Passport Act 2009 and the use of biometric technology.

The principle of due care requires the State to protect the rights and interests of citizens. This implies a serious assessment of the long term effects of biometric applications, including possible unintended side-effects. In view of the observations above about such externalities, this in all probability implies a change in institutional arrangements and policy adaptation.

Prins (1998) also points out that amongst the principles of proper administration, transparency is a vital element in citizen-state relationships, implying opening up the so-called black box of technology. In the case of biometrics, I have previously pointed out that a single and coordinated government view on biometrics is lacking. This lack of coherence and vision undermines confidence and stands in the way of opening this black box.

The principle of legal certainty also poses a challenge to, for example, the Passport Act that introduces a central (biometric) database. The Act is what is called a framework law which is elaborated in significant further detail by 'general administrative orders' that need no parliamentary approval and thus escape the democratic process of formal legislation.

Prins (2007) also holds that sound administration requires more than just the statement of a general policy objective without giving a full insight into any other benefits and effects. In this view, the objective of preventing and combatting fraud as stated in the Passport Act would need further explanation and analysis. In its opinion of 2007 as reiterated above, the DPA notes that the Act has not been accompanied by a proper analysis of the advantages and disadvantages of a central database. The DPA maintains that the principle of due motivation should have been adhered to more properly.[22]

Finally, the proportionality principle, as a vital principle of proper administration, also places a heavy responsibility on the Dutch government. The DPA's call for the Act to be reviewed and its advice that the Act poses a serious infringement of privacy that is not justified by the aims to be achieved, does not sit easily with this principle.

All in all, a reasonable (or due or proper) use of biometrics in Dutch government policy would benefit from closer adherence to the principles of proper administration. The current approach has already been challenged on several of these grounds before a Dutch administrative court.[23] In addition, the civil rights

[22] See the detailed analysis of Hermans 2010 on this subject.

[23] As mentioned above: http://www.nu.nl/binnenland/2185458/student-rechter-privacy-paspoort.html

organization Privacy First has started civil legal proceedings claiming the passing of the Passport Act constitutes a wrongful Act by the Dutch state.[24]

13.7 Conclusion

Based on a quick scan of developments in the private and public sector, we conclude that these Dutch biometric case studies show that practices in handling biometric data blur previous legal and political distinctions. The use of biometrics by the State as a means to uniquely identify citizens, in combination with the current shifts towards a networked state, is affecting the balance in existing power relationships. The collection of biometric data without the existence of a clear and consistent government policy is making the process non-transparent and individual citizens too vulnerable for security and privacy risks and threats.

Due to staff shortage or lack of powers, the Dutch DPA has not been able to develop an active policy on the stimulation of good practice in the use of biometrics. Fieldwork reported elsewhere (De Hert and Sprokkereef 2009a, b) shows that external supervision on the use of biometrics in the private domain in the Netherlands is lacking. The same applies to the public domain. There is also no transparency as to whether and how biometric data are being exchanged between the public and private sector. In view of the increasing trend of government departments and private parties sharing information, the effectiveness of Articles 33 and 34 (obligation to inform) of the Data Protection Act ought to be questioned.

In the evaluation of The Hague program, it is concluded that biometric passports, the second generation Schengen Information System and the Visa Information System will allow increased use of biometrics whilst ensuring that data protection requirements are fully respected (Commission 2009, p. 7). This conclusion is mirrored in the Stockholm program adopted recently as its follow up (European Council 2009). I dare to challenge this assumption. From the developments in the Netherlands, it is clear that the collection and use of biometric data is not counterbalanced by increased possibilities for citizens to correct, withdraw, limit the use or keep control over their information. The security risks involved in biometric data storage and an assessment of the modifications needed to protect citizens are not made public and thus neglected or concealed. Without further measures, the use of biometrics in the information systems of the State will make it more difficult for citizens to defend their interests through the protection of their biometric data.

[24] The organization represents citizens who have refused to provide fingerprints and have been denied a passport as a result, see http://www.privacyfirst.nl/images/stories/PDFs/privacyfirst_20100506_anondagvaardingpasprtwetproces.pdf

References

Commission (2009) Evaluation of the Hague program and action plan, COM (2009) 263 final. Brussels, 10.6.2009

Coordinatiegroep Informatievoorziening Strafrechtsketen (CIS) (2008) Progis: protocol identiteitsvaststelling strafrechtketen. The Hague, Directie Generaal Rechtspleging en Rechtshandhaving, 3 September 2008

De Hert P, Scheurs W, Brouwer E (2007) Machine-readable identity documents with biometric data in the EU—part III—overview of the legal framework. Keesing J Documents Identity 22:23–26

De Hert P, Sprokkereef A (2009a) The use of privacy enhancing aspects of biometrics: biometrics as PET in the Dutch Private and semi-public domain. Tilburg, TILT, January 2009. http://arno.uvt.nl/show.cgi?fid=93109

De Hert P, Sprokkereef A (2009b) Case study The Netherlands. In: Kindt E, Müller L (eds) D13.4. The privacy legal framework for biometrics, Fidis, May 2009. pp 80–93. Also available at http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf

Dijstelbloem H, Meijer A (2009) De migratie-machine: de rol van technologie in het migratiebeleid (The migration machine: the role of technology in migration policy). Van Gennep, Amsterdam

European Council, Stockholm program an open and secure Europe serving and protecting the citizens (doc. 17024/09) adopted on 11.12.2009 (EuCo 6/09)

Grijpink JHAM (2009) Uitgangspunten voor zinvol en veilig gebruik van biometrie. Priv en Informatie 12(6):273–279

Hermans K (2010) Het gebruik van vingerafdrukken voor opsporingsdoeleinden onder de nieuwe paspoortwet en artikel 8 van het EVRM. NTM/NJCM-Bull 35(1):35–40

Hes R, Hooghiemstra TFM, Borking JJ (1999) At face value, on biometrical identification and privacy registratiekamer achtergrond studies en verkenningen, 15 September 1999, pp 1–70. http://www.cbpweb.nl/documenten/av_15_At_face_value.stm

Knopjes F (2009) Verkenning: Op Weg Naar een Visie Op Biometrie, Programma VIPS (Versterking identiteitsketen publieke sector) May 2009

Mordini E, Tzovaras D (eds) (2010) Second generation biometrics. Springer, New York

Prins C (1998) Biometric technology law—making our body identify for us: legal implications of biometric technologies. Comput law secur rep 14(3):159–167(7)

Prins C (2007) Technocratie en de toekomstagenda van de nationale ombudsman. In: nationale ombudsman, werken aan behoorlijkheid. Den Haag, Boom Juridische Uitgevers

Zwenne GJ et al (2007) Eerste fase evalluatie wet bescherming persoonsgegevens: literatuuronderzoek en knelpunt analyse. eLaw@Leiden/WODS

Part IV
Legal Dimensions: EU Law Perspectives

Chapter 14
The Use of Biometrics at the Borders: A European Policy and Law Perspective

Evelien Brouwer

Abbreviations

ECtHR	European Court for Human Rights
SIS	Schengen Information System
VIS	Visa Information System
EDPS	European Data Protection Supervisor

Contents

14.1 Introduction 232
14.2 Migration Control and the Use of Biometrics 233
14.2.1 Eurodac 233
14.2.2 SIS and SIS II 234
14.2.3 VIS 235
14.2.4 Biometrics in Identity Documents and Residence Permits 237
14.3 Extended Use of Biometrics for Law Enforcement Purposes 238
14.3.1 Eurodac 238
14.3.2 SIS II 239
14.3.3 VIS 240
14.4 Right to Privacy Right to Data Protection 241
14.4.1 Biometrics and Interference of the Right to Privacy 241
14.4.2 Necessary in a Democratic Society 242

Contribution received in 2010.

E. Brouwer (✉)
Utrecht University, Utrecht, The Netherlands
e-mail: e.r.brouwer@uu.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_14,

14.4.3 In Accordance with the Law 243
14.4.4 Right to Data Protection: A Fundamental Right 244
14.5 'Strike the Right Balance?' 245
14.5.1 The Value of Impact Assessment 245
14.5.2 European Data Protection Supervisor and National Data Protection Authorities 247
14.5.3 European Parliament 247
14.6 Conclusion 248
References 249

14.1 Introduction

The use of biometrics, including fingerprints and DNA, by governmental authorities is generally associated with the purposes of criminal investigation and law enforcement. More recently, biometrics became a central tool for migration control purposes. Especially at the EU level, different instruments have been adopted on the basis of which fingerprints and facial image of migrants and citizens are collected and stored for identification purposes.

The use of biometrics on the one hand enables national governments to secure identity documents against theft or fraud. On the other hand, it facilitates the search into different databases. In the Communication on the enhanced interoperability and synergies among European databases of 2005, the European Commission promoted the use of biometrics, aside from its use as an identification and verification tool, as a search tool.[1] According to the Commission, biometric searches would allow 'unprecedented accuracy' and 'more accurate identification of wanted persons.' Since 2005, the EU legislator gradually extended or proposed to extend the use of different databases, such as Eurodac and Visa Information System (VIS), primarily meant for immigration control, for law enforcement purposes.[2] The inclusion and extended use of biometrics in these databases resulted in the establishment of a European information system or a system of 'Digital Surveillance' affecting both EU and non-EU citizens, and both regular and irregular migrants. Although in the legislative process, legal standards of privacy, and data protection law have been taken into account, the question remains whether the EU legislator 'struck the right balance' between the objectives of the surveillance systems and the individual rights and freedoms.

In this chapter, the large-scale use and centralized storage of biometrics will be analyzed against the background of the right to privacy as protected in Article 8 ECHR and the EU principles of data protection law. Section 14.2 describes important databases which have been developed in the field of migration control, including the inclusion of biometrics. In Sect. 14.3, it will be questioned, whether these measures are in accordance with the criteria and safeguards of Article 8

[1] Communication of 25 November 2005, COM (2005) 597.

[2] See for an earlier overview Brouwer 2007, pp. 45–66.

ECHR as formulated by the European Court for Human Rights (ECtHR), exploring in particular the meaning of the judgment *Marper* v. *UK*. This section will also refer to the importance of the individual right to data protection which has been laid down in the EU Charter on the Fundamental Rights. Section 14.4 questions the legitimacy of these EU instruments, considering critical comments of important stakeholders, such as the European Data Protection Supervisor, the national data protection authorities, and the European Parliament. This contribution will focus especially on the proposal of the European Commission to extend the use of Eurodac, an EU database including fingerprints of asylum seekers, for law enforcement purposes expressing serious doubts on the legitimacy and proportionality of this measure.

14.2 Migration Control and the Use of Biometrics

This section describes the most important databases (including biometrics) within the field of EU border and immigration control: Eurodac, the Schengen Information System (SIS), and the VIS. The understanding of the initial objectives of these data systems and the (functional and territorial) scope within which these systems are used, and extended to, is necessary to understand their impact on individual rights and freedoms. In Sect. 14.2.4, I will shortly describe the adoption of EU measures on the introduction biometrics in identity documents and travel or residence permits.

14.2.1 Eurodac

Eurodac, operational since 2003, has been the first EU 'Automated Fingerprint Identification System.' It includes fingerprints of asylum seekers and immigrants no younger than 14 years, who applied for asylum in one of the EU Member States or who have been apprehended in connection with the irregular crossing of the external borders.[3] Fingerprints forwarded by the designated authorities of the Member States to the so-called Central Unit of Eurodac may only be used for the aim to establish which Member State is responsible for the application of the asylum request in accordance with the so-called Dublin criteria.[4] By comparing fingerprints of persons applying for asylum with the fingerprints stored into Eurodac, a Member State may check whether this person previously has been in another Member State. This system is based on the presumption that the authorities of each Member State collect the fingerprints of every asylum seeker or every person apprehended in connection with irregular border crossing. Eurodac is not

[3] Regulation 2725/2000 of 11 December 2000 OJ L 316, 15.12.2000.

[4] Regulation 343/2003 (Dublin II) 18 February 2003.

directly accessible by the national authorities: the Central Unit of Eurodac informs Member States whether the fingerprints of a person are in Eurodac, and then by which Member State these fingerprints have been forwarded.

Eurodac does not contain personal information such as name, birth date, or country of origin, but only the fingerprints and an identification number. However, there is no doubt that the person concerned can be easily identified comparing the Eurodac data with the information as recorded into the national files. According to the annual report on 2008, the Central Unit of Eurodac had received in 2008, 357,421 'successful transactions,' meaning each transaction of fingerprint correctly processed by the Central Unit without rejection due to a data validation issue, fingerprint errors or insufficient quality.[5] Of these transactions, 219,557 concerned the fingerprints of asylum seekers. On 31 December 2008, Eurodac held 1,323,363 individual fingerprints.

14.2.2 SIS and SIS II

The SIS is operational since 1995.[6] This database, set up as compensation tool for the abolishment of internal border controls between the Schengen states, included in January 2009, almost 28 million data, of which approximately 1 million alerts on persons. These alerts include persons wanted for arrest or extradition, persons who are searched as witnesses to appear in court, missing persons, and third-country nationals or non-EU citizens to be refused entrance: the majority (currently 80%) of all the persons reported in SIS I concern this latter group.[7] Third country nationals or non-EU or EEA citizens are reported on the basis of national decisions according to which a person is prohibited to remain or stay within the Member State. In principle, a person reported as 'inadmissible alien' into the SIS, shall be refused a visa, entrance, or residence permit for the whole Schengen territory. SIS is accessible by the 27 EU Member States, plus Norway Iceland, and Switzerland. Over the last years, new authorities have been granted access to the SIS, including Europol and Eurojust.

In December 2006, the EU Council adopted Regulation 1987/2006 on the establishment of SIS II.[8] The establishment of the so-called second-generation SIS or SIS II has been justified in order to transform the SIS into a system, technically feasible for a larger group of users. Formally, the new regulation does not change the basic idea of SIS I, giving national authorities access to the central database via

---

[5] Annual report on the activities of the Eurodac Central Unit in 2008, 25.09.2009, COM (2009) 494.

[6] See on the development and meaning of SIS, Brouwer 2008.

[7] This percentage dropped in the last few years because of the introduction and the reporting of the European Arrest Warrant in SIS.

[8] OJ L 381/4, 28.12.2006.

national interfaces. However, the possibility to create links between different categories of data together with the inclusion of biometrics as sole identifier will undoubtedly change SIS II from an investigation tool into a general intelligence tool. Although initially the SIS II Regulation requires the use of photographs ànd fingerprints to confirm the identity of a third-country national who is located on the basis of alphanumeric search of SIS II, Article 22(c) allows that in future, 'as soon as this becomes technically possible' fingerprints may be used as sole identifier.[9] SIS II will then be searchable solely on the basis of fingerprints without the need for further information, such as first name or surname. Under pressure from the EP, the adopted text of the Regulation includes the condition that before this option is implemented, the Commission has to report to the Council and the EP on the availability and readiness of the required technology.

14.2.3 VIS

The Regulation 767/2008 on the establishment of the VIS was adopted by the Council of EU Ministers on 23 June 2008.[10] Whereas initially the VIS database was planned to be operational in 2008, the EU Council set December 2010 as a new target date for the deployment of the system.[11] The purpose of the VIS is to improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities. The exchange of data between Member States on applications and on the decisions relating thereto, should facilitate the visa application procedure, prevent 'visa shopping,' facilitate the fight against fraud, and facilitate checks at external border crossing points and within the territory of the Member States. The VIS will include information on every visa applicant, including his or her biometric identifiers (ten fingerprints and photographs), planning to travel to one of the EU Member States, including the decisions on refusal of visas and issued visas. Furthermore, it will include data on visa applicants and data on persons inviting the visa applicant, each record to be held for five years. When presenting the VIS proposal in 2004, the European Commission estimated that every year 20 million visa applications for the EU would be stored in VIS.[12] In June 2007, when the European Parliament, the

[9] Art. 22(c) reads: 'as soon as this becomes technically possible, fingerprints may also be used to identify a third-country national on the basis of his biometric identifier. Before this functionality is implemented in SIS II, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted.'

[10] OJ L 218, 13.08.2008.

[11] Press Release JHA Council 30 November-1 December 2009, Council document 16883 (Presse 355).

[12] COM (2004) 835.

Council and the Commission reached a political agreement, the Commission stated in its press release that VIS would store information on 70 million visa applicants and would be 'the largest ten fingerprint system in the world.'[13]

On 23 April 2009, the Council and European Parliament adopted in codecision the Regulation 390/2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organization of the reception and processing of visa applications.[14] On the basis of this Regulation, Member States must collect at the moment of submission of the first visa application, biometric identifiers including the facial image and 10 fingerprints. The data collected during the visa application on the basis of this Regulation shall be entered into VIS. This may only be done by duly authorized consular staff in accordance with Articles 6(1), 7, 9(5), and 9(6) of the VIS Regulation. Exempted from the duty to provide biometric identifiers are: children under the age of 12; persons for whom fingerprinting is physically impossible; heads of State or government and members of the national government with accompanying spouses, and the members of delegations (including sovereigns and other senior members of a royal family) when they are invited by Member States' governments or by international organizations for an official purpose. Where fingerprints have been collected from the applicant during an earlier application and were entered for the first time in the VIS less than 59 months before the date of the new application, these data shall be copied to the subsequent application. Access to the VIS is reserved exclusively to duly authorized staff of diplomatic missions or consular posts, however, as we will see below in Sect. 14.3.3, the EU legislator adopted in 2007 a measure extending the access to VIS to other authorities. External service providers are not allowed access to the VIS under any circumstances.[15]

On the basis of Regulation 390/2009, Member States can entrust external service providers with the task of collecting data and applications, including collection of biometric identifiers, and transmitting these applications to the diplomatic mission or consular post. The Member States however, remain responsible for compliance with data protection rules for the processing of data and shall be supervised in accordance with Article 28 of Directive 95/46/EC of the European Parliament, and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Regulation 390/2009 provides that cooperation with an external service provider does not limit or exclude any liability arising under the national law of the Member State(s) concerned for breaches of obligations with regard to the personal data of applicants and the processing of visas. This does not preclude the right of applicants to take direct action against the external service provider under the national law of the third country concerned.

---

[13] Press Release European Commission, 12 June 2007, IP/07/802.

[14] OJ L 131, 29.05.2009. See for the Commission proposal, COM (2006) 269, 31.5.2006.

[15] See further: Geyer 2008.

14.2.4 Biometrics in Identity Documents and Residence Permits

The use of biometrics in EU wide databases is closely connected to the proposals of the European Commission for a European Border Management Strategy of February 2008. This so-called 'Border Package' includes amongst others an entry/exit system, allowing for the electronic recording of the dates of entry and exit of third country nationals into and out of the Schengen area.[16] This entry/exit system would enable national authorities to identify overstayers and to introduce automated gates for 'Bona Fide or Registered Travelers' enabling 'the automated verification of travelers' identity without the intervention of border guards.'[17] For this purpose, the introduction of biometrics in travel documents or passports will enable these 'border machines' to compare them against the biometrics of the traveller, and the biometrics stored into the aforementioned databases, 'accelerating border checks by creating automated separate lanes replacing the traditional control booths.'

In December 2004, the EU Council adopted the Regulation 2252/2004 for security features, and biometrics in passports and travel documents, issued by Member States.[18] According to Article 1 of this Regulation, Member States must include in their passports and travel documents a storage medium containing a facial image in accordance with the security standards set out in the Annex of this Regulation. Furthermore, Member States must include fingerprints in 'interoperable formats.' Although 'interoperable formats' is not further defined, it refers to the requirement of being readable in order, as set out in preamble 2 of the Regulation, 'to establish a reliable link between the genuine holder and the document.' The data are to be secured and the storage medium should have sufficient capacity and capability to guarantee the integrity, authenticity, and confidentiality of the data. According to Article 6 of the Regulation, the digitized facial image had to be implemented into the passports before 28 August 2006 and the fingerprints before 28 February 2008. The scope of harmonization is limited to the security features containing biometric identifiers: the designation of the authorities and bodies that will be allowed access to the data in the storage medium of the issued document, remains a matter of national legislation.

According to the preamble of Regulation 380/2008 on a uniform format for residence permits for third-country nationals, amending Regulation 1030/2002/EC, its purpose is 'solely to set the security features and biometric identifiers to be used

[16] See the Commission's Communication on Examining the creation of a European Border Surveillance System (EUROSUR) and the Communication on Preparing the next steps in border management in the European Union COM (2008) 68, respectively, COM (2008) 69, 13.2.2008.

[17] COM (2008) 69, pp. 5, 6.

[18] OJ L 385, 29.12.2004.

by the Member States in a uniform format.'[19] Based on this Regulation, the residence permits issued by the Member States should include a 'storage medium' for the biometric identifiers: a facial image and two fingerprints 'both in interoperable formats.' In the proposed Annex, it is stated that the residence permit will be produced as a stand-alone document and must be machine readable. It is interesting that during the discussions in the Council, the Estonian delegation explicitly referred to national developments in the field 'e-Government services' for third country national's living legally in the territory by making use of authentication, certification, and digital signature. In response to this Estonian declaration, the Regulation Annex 1 now includes under 'point 16' the option of Member States for the integration of a 'contact chip' into the residence permit.[20] The use of this contact chip is optional but 'must be in line with related data protection rules.' The preamble explicitly refers to the possibility that Member States use the new storage medium to facilitate new technologies such as e-government and digital signature for access to e-services. This proposal is one of the rare examples in which biometrics may be used for more 'positive' actions towards non-EU citizens.

14.3 Extended Use of Biometrics for Law Enforcement Purposes

As we know, the EU legislator adopted several third pillar instruments providing explicitly in the exchange of fingerprints and DNA data of suspected persons between judicial and police organizations in the EU, such as the Prüm Treaty and the Framework Decision on the exchange of police information (Balzaq et al. 2006). In the following section, we will see that 'immigration control instruments,' such as the aforementioned Eurodac, VIS and SIS II are gradually extended for the use of law enforcement and internal security as well.

14.3.1 Eurodac

Although the European Commission already in 2005, pointed to the shortcoming that internal security agencies would not have access to Eurodac, the proposal to make Eurodac accessible by police and law enforcement authorities was officially

[19] OJ L115, 29.04.2008. Note that the original proposal of the European Commission only referred to the 'approximation' of biometric features and identifiers.

[20] The proposed part 16 reads: '16. Member States may incorporate in the residence permit a separate contact chip for national use which shall comply with ISO standards and shall in no way interfere with the RF chip.'

launched by German Presidency in December 2006.[21] This extension was justified, according to the German delegation, because asylum-seekers and foreigners staying in the EU unlawfully would be 'frequently involved in the preparation of terrorist crimes.'[22] The assumption was based on 'the investigations of suspects in the Madrid bombings and those of terrorist organizations in Germany and other Members States' however, has, as we will see below in Sect. 14.1, has never been substantiated with further data.

In 2007, the JHA Council invited the Commission to launch a proposal by which national law enforcement authorities could under certain circumstances have access to Eurodac. This proposal has been presented by the Commission in September 2009.[23] Article 3 of the proposed Regulation contains three material limitations on the intended access by law enforcement authorities and Europol to the data registered into Eurodac. Firstly, the aforementioned authorities may ask for comparison of fingerprint data in Eurodac if a comparison of data stored in national fingerprint databases on the basis of the Prüm Decision (Decision 2008/615) returned negative results. Secondly, the comparison must be necessary 'in a specific case.' Thirdly, there must be reasonable grounds to consider that the consultation of data stored into Eurodac will substantially contribute to the prevention, detection, or investigation of terrorist offenses and of other serious criminal offenses. The comparisons will be carried out through 'verifying authorities' established according to Article 4 of the proposed Decision. In 'an exceptional case of urgency' this verifying authority may receive written or reasoned logged electronic requests and verify only ex-post whether all the conditions for access were fulfilled, including whether an exceptional case of urgency existed. This ex-post verification must take place 'without undue delay after the processing of the request.'

According to the proposal neither the hit nor the data obtained from Eurodac may be transferred or made available to a third country, international organization, or a private entity established in or outside the EU. Member States retain the right to transfer data to third countries to which the Dublin Regulation applies (Norway, Iceland, and Switzerland).

14.3.2 SIS II

Article 27(1) of the SIS II Regulation states that access to data entered in SIS II and the right to search such data directly or in a copy of SIS II data 'shall be reserved *exclusively* (italics EB) for the authorities responsible for the identification of third-country nationals for the purposes of:

---

[21] Council document 16982/06, 20 December 2006.

[22] Council document 17102/06, 22 December 2006, p. 6.

[23] COM (2009) 344, 10.09.09.

(a) Border control in accordance with the Schengen Borders Code[24] and:
(b) Other police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities.'[25]

The latter provision is vague, allowing Member States themselves to decide which 'designated authority' will gain access to SIS II as long this access concerns the coordination of police and customs checks. In addition, Article 27(2) provides for access to SIS II by 'national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.'

14.3.3 VIS

The functions and authorities obtaining access to the proposed VIS were gradually extended during the legislative process. During its meeting of 7 March 2005, the Council adopted the decision that 'in order to achieve fully the aim of improving internal security and the fight against terrorism,' Member State authorities responsible for internal security and law enforcement authorities should be guaranteed access to VIS, 'in the course of their duties in relation to the prevention, detection, and investigation of criminal offenses, including terrorist acts and threats.'[26] A proposal for a decision providing national security agencies and Europol access to VIS was published by the Commission in November 2005.[27] In February 2007, a new proposal of the draft VIS Decision was published changing the explicit reference to internal security agencies in the title and text into 'designated authorities of the Member States.'[28] This definition still may include internal security agencies but, as we already saw with regard to SIS II, implies the risk that national governments also 'designate' other agencies or authorities obtaining access to the VIS. The JHA Council reached agreement on this Decision in their meeting of 12–13 June 2007.[29]

Article 5 of the adopted Decision 2008/633 provides that 'designated authorities' of the Member States may have access to the data on every visa application registered into VIS, including biometrics, under the following three conditions:

---

[24] Community Code on the rules governing the movement of persons across borders. OJ L 105, 13.4.2006.

[25] 5709/6/06. See also the draft of the Austrian Presidency of January 2006 which, for the first time, included this extended use of data on third-country nationals, 5709/06, 27 January 2006.

[26] Conclusions meeting Council Competitiveness 7.III.2005, Council document 6811/05.

[27] See the proposal for a Council Decision concerning access for consultation of the VIS by these authorities, COM (2005) 600 final, 24.11.2005.

[28] Council document 5456/1/07, 20 February 2007.

[29] Press release JHA Council, 12–13 June 2007, Council document 10267/07 (Presse 125), p. 15.

the access must be necessary for the purpose of 'the prevention, detection, or investigation of terrorist offenses or other serious criminal offenses,' the access must be necessary in a specific case, and there must be reasonable grounds to consider that consultation of VIS data 'will substantially contribute to the prevention, detection or investigation of any of the criminal offenses in question.'[30]

14.4 Right to Privacy Right to Data Protection

14.4.1 Biometrics and Interference of the Right to Privacy

Considering case law of the ECtHR, there is no doubt that the current EU measures on systematic collection and large-scale storage of data, including biometrics, fall within the scope of Article 8 ECHR on the protection of the right to private life.[31] For example, in *Amann* v. *Switzerland*, the ECtHR made clear that Article 8 applies to the storage of information relating to an individual's private life by a public authority, regardless of the sensitivity of the data and regardless of the use that is effectively being made by third parties.[32] In this section I will focus on the meaning of the judgment *S.* & *Marper* v. *the UK* for the aforementioned developments. This case concerned the long-term, systematic storage of fingerprints, and DNA samples of individuals, including minors, suspected of having committed criminal offenses, but not convicted. The data were stored into a 'nationwide database with the aim of having it permanently kept and regularly processed by automated means for criminal-identification purposes.'[33] In the judgment, the ECtHR made it clear that fingerprints records constitute personal data containing certain external identification features comparable to photographs or voice samples (para 81). Even if fingerprints are considered as neutral, objective and irrefutable material and, unlike photographs, are unintelligible to the untutored eye and without a comparator fingerprint, the ECtHR found that fingerprints contain 'unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances.' Therefore, according to the ECtHR, they 'are capable of affecting his or her private life and retention of this information without the consent of the individual cannot be regarded as neutral or insignificant' (para 84). Warning against the stigmatizing effect of such

[30] Decision 2008/633 of 23 June 2008 on the access of designated national authorities and Europol to the VIS for the purpose of prevention, detection, and investigation of terrorist offenses and other serious criminal offenses OJ L 218, 13.08.2008.

[31] *Rotaru* v. *Romania*, 4 May 2000, No. 28341/95 ECHR 2000-V, Section 43–44.

[32] *Amann* v. *Switzerland* of 16 February 2000, No. 27798/95, ECHR 2000-II, Sect. 68–70. See for a further description of the ECHR jurisprudence, Chapters 6 and 7 in Brouwer 2008.

[33] S. and *Marper* v. *UK*, 4 December 2008, Appl. No. 30562/04 and 30566/04.

storage, the ECtHR explicitly referred to fingerprints as belonging to special categories of more sensitive data (para 103).

14.4.2 Necessary in a Democratic Society

Dealing with the question whether any interference of the right to private life meets the criterion in Article 8(2) ECHR, 'necessary in a democratic society,' the ECtHR generally leaves a wider margin of appreciation to the national authorities when it comes to national security or the prevention of disorder or crime, than it would in regular cases. However, even when national governments invoke internal security objectives, the ECtHR requires evidence of a substantiated balance of the different interests at stake. Furthermore, the ECtHR requires the availability of procedural guarantees with regard to the scope and time, the specific measures are being used, and also to allow independent courts or authorities to assess the necessity and proportionality of the security measures.

In its jurisprudence on Article 8 ECHR, the ECtHR developed criteria for the necessary balance of powers between the data-collecting authorities on the one hand and the protection of the interests and rights of the individual on the other. Generally, these criteria include: limitations on the exercise of powers to store and use the information; the duty to inform the person concerned in advance with regard to the storage of his or her information; clear definition of the kind of information that may be recorded, of the categories of people against whom surveillance measures may be taken and the purposes for which the information can be used.[34] Although these criteria resemble general data protection rules, it should be underlined that the right to data protection is not synonymous with the right to privacy, and stricter criteria may be applied when the right to private life is at stake. For example, dealing with the scope of protection of Article 8 ECHR, the ECtHR emphasized in *Marper* v. *UK*, the right of every person to be presumed innocent. According to the ECtHR, even if the retention of private data on a person cannot be equated with the voicing of suspicions, nonetheless their perception that they are not being treated as innocents could be heightened by the fact that their data are dealt with in the same way as convicted persons (para 122). In para 124, the ECtHR particularly referred to the especial harmful risks of data retention on minors, considering their special situation and the importance of their development, and integration into society.

Considering the 'necessity' of the measures at stake, the ECtHR considered in *Marper* v. *UK* judgment the relevance of statistics provided by the UK Government to justify their retention of fingerprints and DNA of the applicants. Where the applicants asserted that the statistics provided by the UK government as justification

[34] See also *Segerstedt-Wiberg and others* v. *Sweden*, 6 June 2006, Appl. No. 62332/00. EHRC 2006, 89 annotation J.P. Loof.

for the retention of the data were misleading, the ECtHR affirmed that the figures did not reveal 'the extent to which the "link" with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons' (para 116). Nor did they, according to the ECtHR, demonstrate that the high number of successful matches with crime-scene stains were only made possible through indefinite retention of DNA records of all such persons. Therefore, the statistics in themselves did not establish that the successful identification and prosecution of offenders could not have been achieved by other means, than the permanent and indiscriminate retention of fingerprint and DNA records (para 117). Even if the extension of databases contributes to the detection and prevention of crime, the question remains whether 'such retention is proportionate and strikes a fair balance between the competing public and private interests' (para 118). For this question it is necessary, according to the ECtHR, to investigate the availability of procedural guarantees such as: the availability of time limits, the possibility of the individual to apply for removal or annul his or her data, and whether there is an independent review of the justification of the data retention.

14.4.3 In Accordance with the Law

Jurisprudence of the ECtHR makes clear that for the criterion 'in accordance with the law,' it is not sufficient for the interference with the right to private life to have some basis in domestic law: the law must be accessible to the individual and its consequences must be predictable.[35] Applying this criterion to the different instruments allowing the transfer of biometric data for law enforcement purposes, one must conclude that these measures lack clear and predictable norms. For example, the aforementioned texts dealing with Eurodac, VIS, and SIS II, only provide that the Member States will appoint 'designated authorities' gaining access to the data, without giving any definition or limitation of those authorities. Also considering the fact that more than 27 states and international organizations such as Europol will use these databases, it will be impossible for the data subjects to understand which authority in which country may under which circumstances get access to his or her personal information.

In the *Marper* case, the ECtHR found that the applicable UK law violated Article 8 ECHR, particularly on the grounds that these data were stored for indefinite periods and also because the storage of data on unconvicted persons, including minors, was considered disproportional.

[35] *Huvig and Kruslin* v. *France*, Both cases of 24 April 1990, No. 11801/95, Series A 176A (Kruslin) and No. 11105/84, Series A 176B (Huvig).

14.4.4 Right to Data Protection: A Fundamental Right

The inclusion of data protection as a fundamental right in the Charter on the Fundamental Rights of the EU, made clear that data protection is to be protected as an independent right aside from the right to private life laid down in Article 8 ECHR and 7 of the EU Charter. Since the final ratification of the Lisbon Treaty in 2009, the rights in this Charter must be considered as binding law for the EU and national legislators when implementing or applying EU law. Article 8 of the EU Charter provides:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The extended use of the aforementioned databases, including the use of biometrics, should be in accordance with this right and the standards included in different instruments in the field of data protection, including: the Data Protection Convention of the Council of Europe in 1981, the EC Directive 95/46 on the protection of personal data, the Regulation 45/2001 with regard to the processing of personal data by EU institutions, and the Framework Decision 2008/977 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. In general, these instruments provide for procedural guarantees safeguarding, among other things, the transparency of the use of personal information and databases, and the right of the data subject to obtain information on the data processing in question (purposes, data controller, recipients of information) and the right to access, correction or deletion of his or her information.

Article 13 of EC Directive 95/46 provides that these data subjects' rights may be restricted on the basis of legal exceptions including the need to safeguard national security, defense, public security or criminal investigation. This seems to leave a wide margin of appreciation of national authorities to restrict data protection rights. However, in *Rechnungshof* v. *Österreichischer Rundfunk*, the ECJ clarified that the EC Directive 95/46 must be interpreted in accordance with the right to private life as protected in Article 8 ECHR.[36] In the words of the ECJ, measures or legislation dealing with the processing of personal data incompatible with Article 8 ECHR, would also be 'incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46' (para 91). These latter provisions concern principles and criteria for legitimate data

[36] *Rechnungshof* v. *Österreichischer Rundfunk and Others*, 20 May 2003, Joint Affairs C-465/00, C-138/01 and C-139/01.

processing (including purpose limitation). Furthermore, the ECJ stated that these rights have a direct effect, in the sense that an individual may seek access to a national court in order to prevent the application of national rules contrary to these principles (para 100).

Importantly, when dealing with biometric data and the reliability of these data, is the provision in the EC Directive 95/46 on the quality of data. Article 6(1)(d) provides that personal data must be accurate, and where necessary, kept up—to—date. In the judgment *Huber* v. *Germany*, dealing with the registration of an Austrian citizen in the German central aliens administration or AZR, the ECJ underlined the duty of national authorities safeguarding the quality of data.[37] According to the ECJ, national authorities of Member States must guarantee the accuracy and relevancy of the data being stored 'since a change in the personal situation of a party entitled to a right of residence may have an impact on his status in relation to that right, it is incumbent on the authority responsible for a register such as the AZR to ensure that the data which are stored are, where appropriate, brought up to date so that, first, they reflect the actual situation of the data subjects and, secondly, irrelevant data are removed from that register.'

14.5 'Strike the Right Balance?'

14.5.1 The Value of Impact Assessment

New proposals of the European Commission are accompanied by so-called extended impact assessment studies. These studies include different scenario's, describing the costs and benefits of the legislative or policy options, considering both economic costs, as effects for security or human rights.[38] Although these reports are a valuable contribution to the transparency of the decision-making, the validity of the information being used is not always clear. Also, taking into account different proposals, the final balancing of costs and benefits by the Commission, is sometimes difficult to understand. This may be illustrated with the aforementioned proposal on the extended use of Eurodac.

In the impact assessment accompanying the proposal on extending Eurodac for law enforcement purposes, the Commission provides only marginal information on the usefulness and proportionality of the measure, referring to data from only four Member States (p. 8) concerning the hit rates in cases where the national law enforcement authorities used data files with fingerprints for asylum seekers. These data offer insufficient and outdated evidence of the necessity to give law enforcement authorities and Europol access to the Eurodac data on asylum seekers, as these data do not provide any systematic analysis of the causal relationship

[37] *Huber* v. *Germany*, 16 December 2008, C-524/06.

[38] European Commission 2005.

between the availability of data on asylum seekers on the one hand, and the prevention, detection or investigation of terrorist offenses and other serious criminal offenses on the other hand. This conclusion applies, for example, to the information of the Commission that according to statistical data in Germany in 2006, 19.4% of the crimes were committed by non-nationals, of which 8.5% were asylum seekers. Irrelevant is also the addition that according to these German statistics, of all types of crimes committed by non-nationals 28% related to homicide and manslaughter of which asylum seekers committed less than 14%! The Commission also refers to data provided by the Austrian government according to which in 2006, 19% of recorded crime suspects would have been asylum seekers, however, without taking into account the numbers on asylum seekers who were actually convicted for those crimes. The same conclusion applies to the data provided by the UK government according to which between 2007 and 2008, consultation on the Immigration and Asylum Fingerprint System including fingerprints on asylum seekers produced a hit rate of 7% on counter terrorism. The same problem applies to the data provided by UK authorities according to which between 2007 and 2008 consultation on the Immigration and Asylum Fingerprint System including fingerprints on asylum seekers produced a hit rate of 7% on counter terrorism: no evidence is given on the number of asylum seekers who were actually prosecuted or convicted for terrorist crimes.

According to the Commission, without any action at EU level 'law enforcement authorities will continue to remain ignorant whether or not information on a fingerprint is available at all and in which Member State.' The Commission does not give evidence why measures such as the Prüm Decision and the Framework Decision 2006/960 would not fulfil the necessary requirements for an effective cooperation. By stating that these measures would not work, because this requires the launching of '29 requests for mutual legal assistance with the aim of discovering which, if any, Member State holds data in relation to a fingerprint,' the Commission seems to question the efficiency of these EU instruments for the protection of security and for law enforcement purposes in general.

Furthermore, it is significant that the aforementioned impact assessment only considers the impact of this proposal with regard to the right to data protection, as protected in Article 8 of the EU Charter on Fundamental Rights, but not with regard to the right to privacy, protected in Article 8 ECHR. This seems a significant omission, especially considering the aforementioned case law of the ECtHR making clear that large-scale databases including fingerprints of individuals fall within the scope of this fundamental right. In her explanatory memorandum, the European Commission acknowledges the specific risks of asylum related information. This, for example includes the risk that family members or friends of the asylum seeker may be ill-treated in the country of origin if the applicant's asylum file will leak to the authorities of this country of origin. In the view of the European Commission, the proposal would provide sufficient guarantees against this risk, prohibiting the further transfer of the asylum seekers data to third countries. This conclusion does not take into account the existing bilateral agreements between both EU Member States, as Europol with third states, allowing for further exchange of data.

14.5.2 European Data Protection Supervisor and National Data Protection Authorities

The development of large-scale databases in the EU and the extended use of biometrics in this area have been closely followed by the European Data Protection Supervisor (EDPS) and national data protection authorities. Whereas their comments certainly resulted in extra safeguards and remedies in the adopted legislation, the more principal, serious concerns of the data protection authorities against the measures itself produced less effect. Especially when considering the use and reliance of biometrics, critical comments of important stakeholders seem to have been systematically neglected by policy makers. The EDPS repeatedly warned against the use of biometrics as a 'primary key.'[39] According to the EDPS, since biometrics are always based on probabilities, they will never deliver the unambiguous key that is by definition required for a primary key for databases.

Also with regard to the proposed extension of Eurodac, the EDPS and the national data protection authorities issued critical comments. In his opinion of 7 October 2009, the EDPS expressed serious doubts on the legitimacy of the proposal and the fact that the necessity of the proposal has not been proven.[40] According to Hustinx:

> [T]o be valid, the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing of personal data must be demonstrated. This is all the more required in case of an extensive intrusion in the rights of individuals constituting a vulnerable group in need of higher protection because they flee from persecution.

In September 2009, the national data protection authorities, represented in the Working Party on Police and Justice (WPPJ), stated that the proposal runs counter to fundamental data protection principles such as proportionality of data processing and respect for purpose limitation.[41]

14.5.3 European Parliament

The involvement of the European Parliament during the legislative process on the different instruments described above, resulted in several amendments improving the legal protection of individuals. For example, in both the VIS and the SIS II Regulation, the European Parliament achieved that the personal data may not be transferred to third countries or to international organizations.

---

[39] A 'primary key' can be described as an instrument enabling the identification of a person and, based on this identification, a very rapid search through different databases.

[40] Published on http://www.edps.europa.eu, visited 13 January 2010.

[41] Published on the website of the Dutch Data Protection Authority, CBP, http://www.cbpweb.nl, accessed 13 January 2010.

Also, based on the position of the European Parliament of 10 July 2008 on the draft Regulation on the collection of biometrics for the reception and processing of visa applications, the adopted Regulation 390/2009, now includes an obligation for the Commission to present, three years after the VIS is brought into operation and every four years thereafter, a report to the European Parliament and to the Council on:

- The implementation of this Regulation, including the implementation of the collection and use of biometric identifiers;
- The suitability of the ICAO standard chosen;
- Compliance with data protection rules;
- Experience with external service providers with specific reference to the collection of biometric data;
- The implementation of the 59-month rule for the copying of fingerprints and the organization of the reception and processing of applications.

14.6 Conclusion

The use of biometrics enables national governments to secure identity documents against theft or fraud. It also allows national authorities to use different databases, primarily set up for limited and specified purposes, as investigation or intelligence files. Once biometrical data and corresponding information are available, the risk of their use for other purposes than the ones they were collected for will undeniably remain present. The possibility that the data subject will never be aware of such use is very real.[42] Considering the special position of asylum seekers and their relatives in the country of origin, one could argue that especially with the proposal to extend Eurodac for law enforcement purposes, the European Commission failed to strike a fair balance between the interests of law enforcement authorities and those of the asylum seekers. As mentioned above, in order to meet the requirement of 'necessary in a democratic society' of Article 8 ECHR, the (proposed) measure must be necessary and proportional to the intended goal of the measure. As the ECtHR underlined in the Marper judgment, the use of fingerprints of a particular group of persons for law enforcement purposes, could lead to stigmatization and discrimination of this group of individuals.[43] Considering the registration of fingerprints into Eurodac, it seems not only a disproportional, but also a cynical consequence of this measure that some Member States use advanced technical measures, including X ray research, to estimate the age of a child to find

[42] See also the reaction of the Art. 29 Data Protection Working Party, Opinion on Implementing the Council Regulation (EC) No 2252/2004, 9.

[43] This risk of data collection on a particular group of persons has been confirmed by the German Constitutional Court in the what is called '*Rasterfahndungs* case,' Bundesverfassungsgericht, 4 April 2006, 1 BvR 518/02 published on 23 May 2006.

out whether he or she is already 14 years or older, which is required for his or her registration into Eurodac.[44] One could also refer to the increasing number of asylum seekers arriving in Europe with mutilated fingertips, in order to prevent their deportation to another EU Member State or country of origin. Even if one reasons that these persons decide themselves to mutilate their hands, it is highly questionable whether these consequences of EU measures are 'proportional', when assessing the aims and practical effectiveness of Eurodac.

References

Balzacq T et al (2006) Security and the two-level game: the treaty of Prüm, the EU and the management of threats Brussels. CEPS

Broeders D (2009) Breaking down anonymity digital surveillance of irregular migrants in Germany and the Netherlands. Amsterdam University Press, Amsterdam

Brouwer E (2007) The use of biometrics in EU data bases and identity documents. Keeping track of foreigner's movements and rights. In: Lodge J (ed) Are you who you say you are? The EU and biometric borders. Wolf Legal Publishers, Nijmegen, pp 45–66

Brouwer E (2008) Digital borders and real rights: effective remedies for third-country nationals in the schengen information system. Martinus Nijhoff Publishers, Leiden/Boston

European Commission (2005) Biometrics at the frontiers: assessing the impact on society, report of the joint research centre (DG JRC). Institute for Prospective Technological Studies. ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf

Geyer F (2008) Taking stock: databases and systems of information exchange in the area of freedom, security and justice. Research Paper no 9. Brussels, CEPS

[44] Eurodac Supervision Coordination Group, Second Inspection Report 2009, 24 June 2009, at http://www.edps.europa.eu, pp. 17–19.

Chapter 15
Privacy and Data Protection Aspects of e-Government Identity Management

Brendan van Alsenoy, Els Kindt and Jos Dumortier

Abbreviations

AFIS	Automated Fingerprint Identification System
CNIL	*Commission nationale de l'informatique et des libertés*
CoT	Circle of Trust
DPD	EU Data Protection Directive 95/46/EC
EDPS	European Data Protection Supervisor
Eurodac	European Dactylographic System
ICT	Information and Communication Technologies
IMI	Internal Market Information
PEGS	Pan-European e-Government Services
PET	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification

Contribution received in 2010.

B. van Alsenoy · J. Dumortier · E. Kindt (✉)
The Interdisciplinary Centre for Law and ICT (ICRI), K.U.Leuven, Leuven, Belgium
e-mail: els.kindt@law.kuleuven.be

B. vsan Alsenoy
e-mail: brendan.vanalsenoy@law.kuleuven.be

J. Dumortier
Catholic University of Leuven, Leuven, Belgium
e-mail: jos.dumortier@law.kuleuven.be

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*,
Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_15,

Contents

15.1 Introduction 252
15.2 Application of the Legal Data Protection Framework to e-Government 253
15.2.1 Legitimacy of Processing 253
15.2.2 Finality 254
15.2.3 Data Accuracy 256
15.2.4 Confidentiality and Security of Processing 257
15.2.5 Transparency of Processing and Related Data Subject Rights 261
15.2.6 Determination of Tasks, Responsibilities, and Roles 262
15.2.7 Use of Unique Identifiers 264
15.3 Current Practices 265
15.3.1 Internal Market Information System 266
15.3.2 The Increasing Use of Biometric Data 273
15.4 Conclusion 279
References 280

15.1 Introduction

The European Commission has defined e-government as "the use of information and communication technologies in public administration combined with organizational change and new skills in order to improve public services and democratic processes and strengthen support to public policies."[1] While e-government has a clear potential to improve governmental service delivery and governance, at the same time it gives rise to concerns as to whether these initiatives will not put citizens' privacy at risk. With its development, digital identification, and identity management have become fundamental aspects of public policy, on both a national and a European level. The electronic identities of citizens are in fact at the very center of e-government and the management of their personal information triggers worries and debates as to whether appropriate safeguards are (or will be) in place.[2] In addition, there are certain e-government practices and objectives which augment these concerns. For instance, many European Member States consider "back-office integration" as one of the core objectives of their e-government policy. The eIDM Roadmap developed by the DG Information Society and Media

[1] European Commission 2003, p. 7. E-Government initiatives are being witnessed at all levels of government (local and federal governments, including legislative bodies, the judiciary, the tax administration, in the health sector, etc.). These initiatives can be grouped into four main categories: (1) the disseminating (passive or active) of relevant general public information to citizens, for example through websites, (2) the use of electronic processing and networks to improve the management of activities inside and across governmental departments, (3) the use of ICT to increase citizen participation in decision-making processes (e.g., e-petitions), and (4) the use of ICT for interaction with the citizen and service delivery (e.g., filing of tax return, access to personal file at the National Registry or on an e-health platform, filing of declarations in social security, etc.). For this Chapter, we focus on the activities in group (2) and (4).

[2] See also FIDIS 2008 16.1, p. 17.

of the European Commission goes even further and advocates single collection of personal data.[3] These articulated policy objectives intuitively appear to be at odds with certain established data protection principles, such as the purpose limitation principle and the principle of transparent data processing.

The object of this chapter is to discuss how the current data protection framework relates to the development of e-government. Directive 95/46/EC in principle applies to all personal data processing activities in both the private and the public sector. In case of personal data processing by EU Institutions, Regulation (EC) No. 45/2001[4] must be applied. We do not refer separately to the provisions of this regulation throughout this chapter, seeing as the provisions of Regulation 45/2001, which are relevant to our analysis, are almost identical to the corresponding provisions in Directive 95/46/EC.

We will start by highlighting the implications of several main data protection principles (legitimacy of the processing, finality, data accuracy, confidentiality, and security of processing and transparency). During this discussion we will not only point out areas in which the regulatory framework might be challenged by certain e-government approaches and practices, but also attempt to provide recommendations as to how these challenges might be addressed. After that we will present two case studies. The first case study that will be discussed is the Internal Market Information System, one of the very first Pan-European e-government applications. The second case study will describe some of the choices made by governments in the field of biometrics. Finally, by way of conclusion, we will reiterate our main findings.

Various projects and studies have conducted research in relation to e-government identity management, such as the MODINIS and FIDIS projects.[5] Several of the topics discussed in this chapter rely or build on the results of this research.

15.2 Application of the Legal Data Protection Framework to e-Government

15.2.1 Legitimacy of Processing

The EU Data Protection Directive 95/46/EC[6] ("Directive 95/46/EC" or "DPD") restricts the instances in which the processing of personal data may take place. In particular, Articles 7 and 8 of this Directive enumerate several legal grounds, of which at least one must be present in order for the processing of personal data to be

[3] European Commission 2005, Block VIII.

[4] Regulation 45/2001/EC, L 8/1-22.

[5] See, e.g., Modinis 2006, p. 19; FIDIS D16.1, 2008, p. 143 and FIDIS D16.3, 2009c, p. 88.

[6] Directive 95/46/EC, L 281/31-50.

legitimate (principle of legitimacy of processing). Most relevant to our further analysis is that processing shall be considered legitimate when

- the processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 7, c DPD) or
- the processing is necessary for the performance of a task carried out in public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (Art. 7, e DPD).

A task carried out by government administrations in the public interest is only legitimate if it complies with the three basic principles of public law, namely its (1) legality, (2) speciality, and (3) proportionality (De Bot 2005, p. 37). Article 8 ECHR may impose additional requirements towards the basis of processing according to the European Court of Human Rights, the requirement that the interference must be "provided by law" (legality) refers to the law in its broad ("material") sense and is not strictly limited to statutes or acts. Such legal basis must, however, still be sufficiently precise to allow individuals to foresee its consequences, and to give them adequate protection against arbitrary interference (FIDIS D16.1, 2008, pp. 36 et seq.).

Another basis for legitimacy that merits further discussion is data subject consent (Art. 7, a DPD). Where the individual is actually free to decide whether or not to consent to a particular processing operation, such an approach is often seen as recommendable.[7] The requirement which states that the data subject's consent must be "freely given" (Art. 2, h DPD) may, however, significantly restrict the number of instances in which consent may serve as the basis for the processing for e-government purposes.[8] Even in instances where the citizen can validly express his consent toward the processing, there is by no means an automatic exemption from the requirement of a clear regulatory framework. Additional regulatory initiatives may still be appropriate or necessary depending on the application.

15.2.2 Finality

Article 6, d of Directive 95/46/EC dictates that personal data must be "collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes." This provision embodies the so-called "principle of finality", also known as the "purpose (or use-) limitation principle":

[7] See also European Commission 2005, p. 16 which recommends "maximum"user control within the pan-European eIDM scheme as follows: a mixed voluntary/involuntary data licensing scheme (a stewardship model), whereby the data subject "licenses" access to his personal data to a service provider, either voluntarily or forcibly on the basis of an overriding interest (e.g., emergency health care and national security issues).

[8] In instances where the basis for the processing is found in a regulatory instrument alone, there may be a need to provide additional transparency enhancing mechanisms. See Sect. 15.2.5.

the purpose that is initially specified to justify the collection and/or further processing of the data in principle delineates its authorized usage.[9]

As indicated in the introduction, many European governments consider back-office integration as one of the main functional requirements for successful e-government (FIDIS D16.1, 2008, p. 37). In order to maximize administrative efficiency and to avoid having to repeatedly request the data subject for the same information, several of these governments have introduced the principle of "single collection" into their e-government policies.[10] This approach entails that the citizen's personal data is collected only once and is later shared and re-used by other governmental entities (possibly pending validation of the collected information). As e-government applications continue to be developed, the more applications will make use of a particular piece of information for a continuously increasing number of purposes.

Intuitively, this approach appears to be quite at odds with the finality principle articulated in the beginning of this section. However, Directive 95/46/EC does allow for "re-purposing" of personal data, provided that the subsequent processing operations envisaged in turn meet all the requirements the law ordinarily imposes upon data processing operations (De Bot 2001, pp. 120–121; Léonard 2004, p. 29).[11] In the private sector this would ordinarily require the following steps: providing (additional) notice to the data subject of this new purpose (re-)obtaining an informed consent, additional notification to the data protection authority, etc. In the e-government setting this will mainly entail adopting new (or expanding existing) legislation and obtaining authorization from national data protection authorities (where applicable).[12]

When scrutinizing the "compatibility" of these distinct processing operations, the evaluation should not, however, be limited to the finding of a legal basis warranting the processing. In addition, the reasonable expectations of the data subject, the nature of the data processed, and the possible prejudices toward the data subject must also be taken into account. This follows not only from the language of the Directive, but also from the obligations of Member States under Article 8 of the European Convention of Human Rights and Articles 7 and 8 of the EU Charter of Fundamental Rights (FIDIS 2008, pp. 36–37). So-called "Privacy Impact Assessment" (PIA) models may be useful tools to help ensure that sufficient consideration is given to the re-purposing of personal data within e-government.[13]

---

[9] See, e.g., Article 29 EHR Article 29 2007a, p. 6; Bygrave 2001; Kosta and Dumortier 2007, p. 133.

[10] See, e.g., Deprest and Robben 2003, p. 7.

[11] See also FIDIS 2008, pp. 36–37.

[12] For instance, a prior authorization scheme was introduced in Belgium, *inter alia*, to help mitigate some of the risks associated with use of a single unique identifier. See http://www.privacycommission.be/en/sectoral_committees for an overview of the sectoral committees which are charged with granting or denying prior authorization for access or use of certain governmental databases and/or identifiers.

[13] See also FIDIS 2008, p. 46.

15.2.3 Data Accuracy

Every data controller is under the obligation to ensure the accuracy of the personal data it processes (Art. 6, d DPD). In order to achieve data accuracy within e-government applications, several Member States rely on what can be characterized as "authoritative sources".[14] An authoritative source can be described as an entity that is functionally responsible for the collection, validation, and updating of data and which is recognized as being the most accurate and up-to-date source of such information (FIDIS D16.3, 2009c, pp. 17–18). The designation of authoritative sources essentially involves determining which entities are authorized to act as data providers for which data items or data sets. In order to ensure that the information being maintained is in fact reliable, the designation of an authoritative source should be accompanied by appropriate policies specifying how the data will be collected, validated, and kept up-to-date. These policies should also specify the measures that shall be used to prevent unauthorized modifications or entries.[15]

In order to ensure the availability and to enable the exchange of data among governmental entities, this model typically relies on the implementation of so-called "reference directories". These tools do not store the actual content of the data as such, but rather provide "pointers" as to the logical location from where the information may be retrieved. "Discovery services" in turn allow authorized users to locate resources within a network, including services and entity information such as credentials, identifiers, and attributes.[16]

The use of authoritative sources is typically justified by the advantages of having single points of contact to update and manage information. Specifically, this approach helps to avoid the existence of multiple copies of the same information in different databases, among which discrepancies may start to develop over time. From a policy perspective, it can also be seen as a natural extension of the principle of "single collection" referenced above.

---

[14] See FIDIS D16.1, 2008, p. 45. In many documents these authoritative sources are also referred to as "authentic sources" or "authentic registers". We have chosen to use of the term "authoritative" as it is more in line with identity management literature and because we believe the term "authoritative" better captures their actual role (it reflects the idea that they are seen as trustworthy within a certain context). Moreover, use of the term "authentic" may also in the long run engender confusion with notions such as "authentication" or "data authenticity" in the way traditionally used in computer sciences. On the use of "authenti" sources as part of the pan-European eIDM framework, see European Commission 2005, p. 5.

[15] See also FIDIS D16.3, 2009c, p. 19.

[16] Based on ITU-T 2007, p. 18, available at http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html. See also FIDIS D3.17, 2009a, for a description of how reference directories have been implemented within Belgian e-government.

From a privacy perspective, the use of authoritative sources may help to minimize the amount of data stored centrally, which may in turn reduce the potential gain for attackers. They may also be said to advance the principle of data minimization; in the sense that their use can help to avoid unnecessary duplication of the same data. Furthermore, the use of authoritative sources arguably, also increases the probability that the most accurate information is being processed, provided of course that it is sufficiently validated and updated in due time (FIDIS D16.3, 2009c, p. 18).[17] The outlined approach, however, also entails its own set of privacy risks, which should be considered carefully when developing an e-government framework in accordance with this model. Although the data no longer needs to be maintained centrally, the implementation of such tools and services in turn creates centralized data aggregation opportunities. For this reason, careful consideration should be given as to which entities are charged with maintaining, managing, and operating data registries and reference directories. Such roles should in principle only be bestowed upon independent intermediaries that have a clear statutory obligation to ensure policy compliance for the transactions they process. Ideally, these entities would operate under close supervision of national data protection authorities and be subject to regular audits. E-government developers should also consider maintaining some form of functional separation among the entities that manage directory services, e.g., by taking into account the different contexts and sectors (such as health, finance, social security, etc.). Each intermediary should of course then only manage references to the extent that there are legitimate bases warranting retrieval and exchange of this information (FIDIS D16.3, 2009c, pp. 18–19).

15.2.4 Confidentiality and Security of Processing

Articles 16 and 17 of Directive 95/46/EC obligate the data controller(s) of a processing operation to implement appropriate technical and organizational measures to ensure the confidentiality and security of processing. In particular, controllers must adopt such measures to "protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing." The controller's security obligation may be qualified as an obligation of means. There are four criteria for determining the extent of this obligation, namely state-of-the-art, cost, the risks presented by the processing, and the nature of the data to be protected (Art. 17, 1 DPD).

[17] See Belgian DPA Belgian 2008, p. 4.

Several national data protection authorities have issued guidelines as to the types of organizational and technical measures data controllers should consider when handling personal data.[18] In the following paragraphs we will briefly elaborate further on a number of specific aspects of the controller's security obligation and in particular upon certain technical measures which merit further discussion in the context of e-government identity and information security management.

"Confidentiality" as a security objective is understood as keeping the content of information secret from all entities except those that are authorized to access it (Huysmans and Van Alsenoy 2007, p. 12). There are numerous approaches to providing confidentiality, ranging from physical protection to the use of access control and cryptographic algorithms (Menezes et al. 1997, p. 32). In addition to safeguarding the confidentiality of information, the processing capabilities (read, write, modify, etc.) of each entity should be limited to that which is necessary to realize the goals of the processing. This follows from a combined reading of the controller's security obligation and the proportionality principle. These requirements apply not only at the level of each governmental entity, but also at the level of each individual user (FIDIS D16.3, 2009c, p. 20).

In order to manage the permissions of the individual entities within an e-government network, EU Member States have developed (or are starting to develop) an identity and information security management framework for their applications. A first step in the development of such a framework involves putting in place reliable identification and authentication mechanisms. To this end, more and more Member States have moved from purely paper-based identification documents toward identity cards which also enable identification and authentication in a digital environment, in most cases based on Public Key Infrastructure (PKI).[19] In several instances these electronic identity cards have also been equipped with cryptographic functionalities which enable the cardholder to place qualified electronic signatures within the meaning of Directive 1999/93/EC on a Community framework for electronic signatures.[20]

In addition to the deployment of reliable identification and authentication mechanisms, e-government developers must also incorporate into their applications, appropriate privilege and authorization management mechanisms. Prior to setting up a particular e-government application, the available resources and services need to be documented. The personal data contained in these resources

[18] These guidelines are typically adaptations of (or have been clearly inspired by) standards of the ISO/IEC 27000 Series (Information Security Management) (formerly known as ISO 17799 or BS 7799). See, e.g., Belgian DPA Reference measures.

[19] See IDABC 2007, pp. 72 et seq. For transactions which only require a low level of entity authentication assurance, alternative mechanisms such as username–password combinations and other non-PKI-based tokens are also accepted. See also Hulsebosch et al. 2009, p. 44.

[20] Directive 1999/93/EC, L 13/12-20. The Belgian electronic identity card for instance, incorporates this functionality. For an overview of all the functionalities of the Belgian eID card, see Van Alsenoy and De Cock 2008, pp. 178–183.

should also be categorized in a generic fashion (e.g., contact data, age, social security status, etc.). After an overview has been made of which types of information are needed for a particular application, the business processes and information flows must be mapped out so that the exact function and role of each possible user can be clarified. The access and processing capabilities of each entity can then be determined, but must be defined according to that which is strictly necessary for the requirements of the application or service (cf., *supra*). This should enable an overview of authorized recipients for each data element that qualifies as personal data, as well as a list of the actions they are allowed to perform upon these resources (FIDIS D16.3, 2009c, p. 20).

When considering the scale of e-government applications, it is important to think of privilege management not only at object or user level, but also at policy level (FIDIS D16.1, 2008, p. 22). In other words, technical policy enforcement mechanisms should not only be thought of in terms of a role-based access control model. Policy enforcement should also comprise rules and conditions which allow verification that the prerequisite attributes, which the entity attempting to perform a particular action should possess, are in fact present at that moment. After all, the actual authorization profile of an individual user (i.e., the entirety of actions he or she is allowed to perform) is often premised on the attributes associated with him or her which may vary over time. For instance, the privileges which should be accorded to a user may be dependent on professional qualifications (e.g., health professional, attorney), membership of a group (e.g., employee of a particular governmental agency), or mandates (e.g., from a citizen to his accountant), which may become revoked or expire.[21] When designing a new application, developers should then carefully consider precisely which attributes need to be present to justify authorization.[22]

Policy rules can naturally also incorporate other conditions than just attributes, such as the existence of a prior authorization issued by the national data protection authority.[23] Where such a prior authorization scheme exists, it is recommendable that the technical policy enforcement mechanisms that are used, also have the ability of verifying whether or not such a prior authorization has been issued. This of course requires that the authorizations (or legal exemptions thereto) are

[21] FIDIS D16.3, 2009c, p. 18. For a detailed description of how mandates from citizens to their accountants are managed in the Belgian "Tax-on-Web" application, see Van Alsenoy et al. 2009, pp. 418–419. See also FIDIS D3.17, 2009a, pp. 46–49 (also describing the use of authoritative sources as part of user and access management within Belgian e-government). On this last point see also FIDIS D16.3, 2009c, pp. 18, 20.

[22] See also Deprest and Robben 2003, p. 45 and Belgian DPA 2008, p. 9.

[23] For instance, a prior authorization scheme was introduced in Belgium, *inter alia*, to help mitigate some of the risks associated with use of a single unique identifier. See http://www.privacycommission.be/en/sectoral_committees for an overview of the sectoral committees which are charged with granting or denying prior authorization for access or use of certain governmental databases and/or identifiers.

systematically updated into the system's policy information points in order to maintain the functionality of the system (FIDIS D16.3, 2009c, pp. 20–21).[24]

Access control policies play a crucial role in protecting the confidentiality of information. However, they are generally limited to challenging a requesting entity to produce the appropriate credentials and subsequently evaluating its processing rights in light of the applicable policy. On the other hand, data are most often transmitted across public networks, which introduces additional security risks (interception, man-in-the-middle attacks, etc.) that cannot be resolved by access control policies alone. Encryption is a technique which transforms data from a readable form (known as plain text or clear text) to one that is unintelligible (referred to as cipher text). It may be applied during transmission as well as during storage. This helps to maintain confidentiality even in instances where data has been intercepted or the security of a database has been compromised (FIDIS D16.3, 2009c, p. 24).[25]

Confidentiality is only one of the many security aspects which need to be addressed by data controllers. In order to avoid unauthorized destruction or alteration, the information security management system should also integrate appropriate security policies to safeguard the integrity and authenticity of the data. In order to ensure data accuracy, a sufficient level of certainty must exist as to the identity of the information provider. Parties involved in an exchange must be able to establish whether the information emanates from an authoritative and authorized source (FIDIS D16.3, 2009c, p. 24). The integrity and authenticity of data in transit should be appropriately protected, e.g. through use of data origin authentication protocols (which also serve to establish their integrity during transmission). Relying parties should only be permitted to process personal data further if there is sufficient certainty as to its origin and integrity (i.e., upon verification that it emanates from the intended source and has not been subject to manipulation) (FIDIS D16.3, 2009c, p. 24).

Not all data processing requires the same level or type of protection. Information security management frameworks should distinguish between processing operations according to the specific risks they present, to help determine which security properties are relevant in which instance and to identify the appropriate safeguards.[26]

---

[24] As a rule, the more granular the technical policy enforcement mechanism, the more risks of unlawful data processing can be ruled out. By narrowly tailoring the access and processing capabilities of individual users, there should be a greater likelihood of compliance with the proportionality and legality principle. Some technical policy enforcement mechanisms can even be configured to take into account the purpose of a request, which can in turn help to limit excessive processing capabilities for a particular operation, as well as facilitate later compliance verification. When purpose does become part of the technical policy information, sufficient safeguards must be implemented, as such information may often prove to be sensitive in and of itself. See also FIDIS D16.3, 2009c, p. 21.

[25] For more information on encryption schemes see ibid., pp. 37 et seq.

[26] An example of a risk-based approach toward the protection of the confidentiality of personal information can be found in McCallister et al. 2009.

15.2.5 Transparency of Processing and Related Data Subject Rights

Articles 10 et seq. of Directive 95/46/EC set forth the controller's obligations of transparency and list the rights data subjects can exercise toward controllers when their personal data is being processed. Underlying these provisions is the idea that the data subject should in principle be notified of the processing of his personal data (notice),[27] should be provided with tools to obtain further information (right of access),[28] and should also have immediate means of recourse toward the controller in case he feels his data is being processed improperly (right to rectification, erasure, or blocking).[29]

The transparency of processing can be seen as a necessary antecedent for the data subject in order to exercise the rights as a data subject: if the subject is not aware of the processing, he will not be able to scrutinize the processing and make a determination as to whether or not to object to the processing, or whether he wishes to submit a request to see his data amended, etc. When looking at the exceptions to the notice requirement contained in Article 11 DPD (indirect collection), it is noteworthy that the data controller is exempted from this obligation, *inter alia*, in the following two instances.

- When the recording or disclosure is expressly laid down by law.
- When data is collected indirectly and informing each data subject would involve a disproportionate effort.[30]

These limitations cover a large part of e-government data processing, particularly where single collection and reuse are considered core policy objectives. It could therefore be argued that they *de facto* abolish the requirement of transparent data processing for e-government applications.[31] Where data processing is based on legislation alone, of which the average citizen may not be knowledgeable, there is a reasonable probability that many citizens will remain completely unaware of the processing (until they are directly confronted with its effects).[32] Therefore, consideration should also be given to implementation of transparency-enhancing mechanisms, particularly in instances where the basis for the processing is not found in the consent of the data subject but rather in a regulatory instrument.[33] Article 11, 2 DPD explicitly calls upon Member States to implement "appropriate

[27] Arts. 10 and 11 DPD.

[28] Art. 12, a DPD.

[29] Art. 12, b DPD.

[30] Art. 11 DPD.

[31] See Papakonstantinou 2001, p. 52.

[32] See also FIDIS D16.1, 2008, p. 40.

[33] Cf., Sect. 15.2.1. When the processing is based on user consent or the data are otherwise collected directly from the data subject, the latter will as a rule be provided with notice in accordance with Art. 11, 1 DPD.

safeguards" with regard to transparency when information is not directly collected from the data subject.

Several Member States have developed "best" or "good" practices aimed at enhancing transparency of e-government operations toward citizens. For instance, in Belgium, the "My File" application enables citizens to not only view their personal data maintained in the databases of the National Register, but also to see which governmental entities have accessed this information.[34] A major added value of such applications is that they also provide *ex post*- transparency. Furthermore, they may also reduce the administrative burden associated with right-of-access requests, provided of course, all the information stipulated in Article 12, a DPD is in fact made available. This approach can also have a added value with regard to the accuracy of the data being processed, as the individuals concerned are often best placed to report suspected inaccuracies.[35]

15.2.6 Determination of Tasks, Responsibilities, and Roles

In the preceding sections we have elaborated upon several of the major principles underlying data protection and briefly discussed how they relate to the context of e-government. Ensuring compliance with these and other data protection requirements across all actors involved in e-government applications is not an easy task. E-government applications typically involve collaboration among a large number of disparate entities. For such collaboration to be successful, agreements need to be made regarding the exchange of identity information among the communicating entities. Such a form of cooperation resembles what has been described in identity management literature as a "Circle of Trust" (CoT), which can be described as an association compromising a number of service providers and identity providers whereby members have agreements in place regarding how identity information should be managed.[36]

---

[34] See http://www.mijdossier.rrn.fgov.be; http://www.ibz.be/download/press/Europe_E-gov_Awards_Good_practice_Mon_dossier-NL.pdf (accessed 3 April 2009). See also Millard 2007, pp. 35–36. In its current form the "My File" application is limited to the data maintained and accessed at the level of the National Register alone.

[35] See also Millard 2007, p. 36. Such an approach can also be brought inline with the seventh Building Block of the pan-European eIDM Framework: "Data control also implies active involvement in issuing, extending, restricting and withdrawing of credentials; and in management of personal data (including accessing and updating personal data to a maximum extent), in order to ensure that data in official authentic sources remain as accurate as possible" (European Commission 2005, p. 16).

[36] FIDIS D16.3, 2009c, p. 13. See also Roessler 2002, pp. 33 et seq. This term originates from the Liberty Alliance (www.projectliberty.org), a standardization body which develops specifications primarily for federated identity management systems. The term is used more broadly, as to encapsulate the essential components of an e-government framework. See also FIDIS D16.3, 2009c, pp. 13–15.

While the basic foundation of a CoT is the reaching of an agreement on how identification and authentication of users will be organized, there are many additional tasks which need to be allocated within an e-government framework in order to ensure compliance with both legal and policy requirements. The following is by no means an exhaustive list of several of the tasks and responsibilities which will most likely need to be considered (FIDIS D16.3, 2009c, p. 17).

- Which entities are authorized to act as data providers for which data sets (i.e., act as authoritative sources; cf., *supra*, Sect. 15.2.3);
- Which entities shall perform which authentications, authorizations, and checks;
- Which entities will be charged with the maintenance of logs for which operations[37];
- Which entities shall act as trusted parties (e.g., intermediaries) to which transactions;
- Which entities will be charged with the updating of technical policies;
- Which entities shall serve as a front-office to accommodate the rights of data subjects such as the right of access and correction;
- Which entities shall serve as a point-of-contact in the event of a security breach;
- Which entities shall be charged with regular verification of policy compliance (audit);

From a data protection perspective, these tasks need to be allocated primarily to ensure the confidentiality and security of processing (Arts. 16–17 DPD; cf., *supra*, Sect. 15.2.4). From a business or policy perspective, such task allocation is required in order to ensure stakeholder trust in the infrastructure and to prevent processing operations from taking place in a way that is detrimental to the interests of the participants.

Directive 95/46/EC sets out certain roles to which it attaches certain responsibilities. In an e-government setting, any participant (service provider, identity provider, intermediary, and authoritative source) might be acting as a controller, processor, or third party, depending on the application at hand (FIDIS D16.3, 2009c, p. 16). When a law mandates a certain form of processing, it should indicate which entity shall act as a controller. Where legislators are not explicit in this regard, but merely entrusts the processing to a particular governmental entity, it may be assumed that the latter will be responsible for the processing operations it performs pursuant to this legal basis (De Bot 2005, p. 35).

However, there may still be instances in which the qualifications of "data controller" *versus* "data processor" are difficult to make. For instance, several governmental entities might be charged with complementary tasks of public interest. This, in turn, might require multiple governmental entities, each within their respective domain, to carry out certain processing operations. If there is no clear specification in the law as to which entity shall act as a controller, their

[37] See also Belgian DPA Belgian 2008, p. 3.

respective roles are determined by the general criteria of the Directive (purposes, means).[38] In any event, the collaborating entities should have a clear understanding as to which entity will take up which role with regard to each processing operation and determine how compliance with the respective obligations shall be ensured in each instance (FIDIS 16.3, 2009c, p. 17).[39]

15.2.7 Use of Unique Identifiers

The use of national unique identifiers within e-government has been the topic of much debate. The intensity of these debates and their outcome at the national level, however, differs significantly among EU Member States.[40] In certain countries, laws introducing such national identity numbers have been successfully challenged in court on constitutional grounds and in at least one case even excluded in the constitution, such as in Portugal.[41] In other countries this issue has not triggered much public debate at all (e.g., Belgium).[42]

Article 8.7 of Directive 95/46/EC provides that "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed." Every Member State has since defined its own "identifier policy", among which there exist substantial differences. In its Working Document on E-Government of 2003, the Article 29 Data Protection Working Party presented the existing "state of affairs" on the use of sector-specific *versus* single identifiers in national e-government systems.[43] The document itself, however, does not provide a thorough analysis of the privacy concerns related to the use of unique identifiers.

A great deal of the research into Privacy Enhancing Technologies (PETs) of recent years has focused on developing mechanisms and tools to limit unwanted correlation possibilities ("linkability") among digital identities and transactions. The central underlying notion appears to be that, where individuals are

---

[38] See Art. 2, d DPD.

[39] In Sect. 15.3.1, we shall describe how the European Commission has addressed this issue in the context of the Internal Market Information (IMI) system; cf., *infra*.

[40] For instance, in France, the plans of the government in the 1970s to identify the citizens by a number and to use this number in all sectors of the public administration [the so-called plan SAFARI "'Système Automatisé pour les Fichiers Administratifs et le Repertoire des Individus" of 1974] in fact led to the adoption of the data protection legislation of 1978 and the installation of the "Commission nationale de l'informatique et des libertés" ("CNIL"). About this project, see also CNIL, Un peu d'histoire, available at http://www.cnil.fr/index.php?id=16

[41] See references to a Hungarian Constitutional Court case of 1991 and Portugal in EPIC 2007, p. 25.

[42] See De Bot 2005, pp. 61–62.

[43] Article 29 eGov 2003, p. 18. The Article 29 Data Protection Working Party hereby relied on answers to a questionnaire submitted to the national data protection authorities relating to e-government issues.

consistently identifiable in the same manner, this may create (or at least facilitate) opportunities for unlawful data exchange, data aggregation, and profiling.[44]

The EC eIDM Roadmap has underlined the need for "the consistent use of suitable identifiers" (European Commission 2005, p. 4). Unique identifiers are in fact an inevitable part of any eIDM framework. The major concerns with regard to personal identification numbers, however, do not relate to the usage of a unique identifier as such, but rather to the use of the same identifier across a multitude of contexts and/or sectors.[45] These concerns magnify themselves when the eID tokens, the government issues to its citizens, are also intended for private sector uptake and the corresponding identifiers are propagated indiscriminately (Van Alsenoy and De Cock 2008, pp. 181–182).[46]

Multiple alternative models have been explored in both research projects and standardization fora and have even become a component of several commercial applications. It is not the purpose of this contribution to describe in great detail the possible alternatives to the use of single national identifiers in e-government, nor to issue a specific recommendation as to what would constitute an appropriate model. We do, however, strongly recommend that this issue be the object of further consideration, research, and debate. Such further consideration appears to be required not only from a privacy perspective, but also from an interoperability perspective. The advent of Pan-European e-Government Services (PEGS) has made clear that the divergent opinions with regard to what constitutes appropriate use of national identification numbers may create an obstacle to the development of interoperable PEGS.[47]

15.3 Current Practices

In this section, two examples of how the e-government initiatives have developed over recent years are discussed. The first example relates to the Internal Market Information System, while the second discusses the use of biometric identifiers in a number of applications.

---

[44] For a more detailed overview of the privacy risks that may emerge when systematic recourse is made to the same identifier across contexts and sectors (in particular when identifiers are propagated and used beyond the domain of applicability for which they were originally intended), see Van Alsenoy and De Cock 2008, pp. 180–181. See also FIDIS D16.1, 2008, pp. 43–46.

[45] See also FIDIS D13.3, 2007b, p. 23.

[46] See also Schreurs and De Hert 2005, pp. 6, 10.

[47] See Modinis 2007, p. 45 and Leenes et al. 2009, p. 40. Closely related to this issue are the current obstacles caused by national authorization schemes which have been put in place as an additional safeguard towards the use of national identifiers (e.g., in Belgium). The latter issue is unlikely to be resolved before an agreement can be made among all Member States on how personal identification numbers should be treated in the context of PEGS.

15.3.1 Internal Market Information System

The IMI system is an ICT tool designed to facilitate information exchange among Member States. In particular, IMI aims at providing support for the practical implementation of Community acts that require an exchange of personal data between Member States' administrations. Currently IMI is aimed only at facilitating information exchange in the furtherance of internal market legislation,[48] but it is envisaged that its use will be expanded to a number of areas in the future.[49]

The IMI project officially started in 2005 in the context of the IDABC program.[50] In the first version of the application, a test pilot was implemented supporting information exchange with regard to four professions governed by the Professional Qualifications Directive (accountants, doctors, pharmacists, and physiotherapists). In the second phase, this version of the application has been expanded to support more functionality and additional professions. In phase 3, further development is being carried out in order to extend IMI to support the Services Directive.[51]

In essence, the IMI system is currently structured as a network which allows the "Competent Authority" of a given Member State to identify its counterpart in another Member State and to exchange information using the IMI network. In addition to its search function, IMI provides users with a set of pre-translated menus, as well as standardized questions and procedures to support the information exchange. All functionality of IMI is accessible via web pages.[52]

In its current version, IMI is aimed mainly at providing national administrations with support in determining the authenticity and scope of credentials presented by an EU citizen from a different Member State. One of the examples provided in the Commission's Data Protection Guidelines is quite illustrative in this regard.[53]

> A German doctor resident in Berlin marries a French man and decides to start a new life in Paris. The German doctor wants to practice her profession in France and therefore submits titles and diplomas to the Order of Doctors in France. The person dealing with the file has doubts about the authenticity of one of the diplomas and uses IMI to check with the competent authority in Berlin.

The IMI network can in a sense be seen as a "federation" of authoritative sources for specific attributes, currently qualifications needed to exercise a

---

[48] Such as Directive 2005/36/EC, L 255/22-142.

[49] EDPS 2007, C 270/1-7, consideration 2. The Annex of Commission Decision (2008/49/EC) lists the relevant Community acts on the basis of which information can be exchanged (currently listing only Professional Qualifications and Services Directives). When new legislation is adopted which provides for information exchange using IMI, the annex will be updated simultaneously (Ibid., consideration 9).

[50] See also http://ec.europa.eu/idabc/en/document/5378/5637 (accessed 22 July 2009).

[51] See http://ec.europa.eu/internal_market/imi-net/about_en.html (accessed 22 July 2009).

[52] See Article 29 IMI Article 29 2007b, p. 4.

[53] European Commission 2009, L 100/12-28.

particular profession or provide a particular service.[54] The IMI system itself thereby acts as an intermediary. It provides a platform through which a relying party (receiving country) may request corroboration of a particular attribute (prerequisite qualification) with the relevant attribute authority in another Member State (country of origin). In this sense the IMI system itself can also be thought of as providing one of the first discovery services for PEGS (with the understanding that the information retrieval and exchange at this time does not yet take place in a fully automated fashion, but still requires a substantial amount of human intervention).[55]

Now that we have outlined the main functionalities of the IMI system, we will proceed with a brief analysis of the main steps that have been taken to ensure compliance with the data protection requirements elaborated in the preceding sections. Keeping in mind that several aspects of this compliance framework are still under development, our analysis shall, where appropriate, make brief reference not only to the current framework, but also to the instruments and opinions which preceded it.

15.3.1.1 Definition of Roles and Responsibilities

As we elaborated earlier, the cooperation among autonomous governmental entities requires a clear understanding as to which entity shall assume responsibility for which task, including a specification of how compliance with data protection requirements shall be ensured. We also highlighted the need for a determination as to which entity shall be considered to act as a controller in which instance, and that this should be clearly indicated within the regulatory framework.

The first effort toward defining the various responsibilities and roles of the actors involved with regard to data protection requirements was made in Commission Decision 2008/49/EC.[56] This effort was not received entirely well by the European Data Protection Supervisor (EDPS).[57] Specifically the EDPS stated that the allocation of roles and responsibilities in Article 3 of Decision 2008/49/EC was

[54] One should note, however, that IMI currently does not incorporate national eIDM products in any way: IMI users are provided with credentials (username/passwords/roles) through their national coordinators and local administrators. In this sense the IMI model differs from typical federation models, whereby the mutual reliance on various identity providers is a key aspect. Though managed in a distributed fashion, there is in fact a "centralized" rather than federated IdP model for IMI (only attribute authorities are "federated").

[55] Upon receipt of a request directed through IMI, the relevant Competent Authority will query its own databases in order to return the appropriate response and manually insert the response (no direct access to local databases managed in other Member State is provided).

[56] See European Commission 2007b, L13/18-23, in particular Art. 3 and Arts. 6–10. Recital 5 in fact provides: "Since the various tasks and functions of the Commission and the Member States in relation to IMI will entail different responsibilities and obligations as regard data protection rules, it is necessary to define their respective functions, responsibilities and access rights".

[57] See in particular EDPS 2007, considerations 10 and 34.

unclear and ambiguous and that several additional specifications needed to be made, namely that[58]

- 'Each Competent Authority and IMI coordinator is a controller with respect to its own data processing activities as a user of the system.
- The Commission is not a user, but the operator of the system, and it is responsible, first and foremost, for the technical operation, maintenance, and ensuring the overall security of the system and that.
- The IMI actors share responsibilities with respect to notice provision and provision of right of access, objections, and rectifications.' (cf., *infra*, Sect. 15.3.1.4).

These specifications provided by the EDPS have since then been integrated in the recently issued EC Recommendation on data protection guidelines for IMI.[59] While very useful as initial guidance, these additional specifications do not yet by themselves provide a comprehensive overview of the respective roles and responsibilities with regard to any specific processing activity within IMI. It does, however, provide an appropriate foundation upon which further specifications may be developed.[60]

15.3.1.2 Legitimacy of Processing

With regard to the legal basis of the processing, the Commission relied primarily upon Decision 2004/387/EC (the "IDABC" decision),[61] in particular Article 4 thereof; in combination with the Professional Qualifications Directive and the Services Directive. Both the Article 29 Working Party and the EDPS have expressed multiple reservations as to the adequacy of these instruments toward ensuring the legitimacy of processing.[62]

In its opinion of Article 29 2007b, the Article 29 Working Party recommended that the Commission adopt an "ad hoc" solution to support the existing legal basis in the form of a Commission Implementing Decision.[63] Decision 2008/49/EC "concerning the implementation of the Internal Market Information System (IMI) as regard the protection of personal data" was adopted in response to this recommendation.[64] Despite this measure, the EDPS has continued to express its

[58] EDPS 2007, consideration 35.

[59] European Commission 2009, L100/17.

[60] While the respective roles have been clarified at least so as to allow determination in the event of a dispute, the cooperation among the participants of IMI in order to ensure "end-to-end" compliance, in particular task allocations, still appears to require further work. This aspect will become more apparent in the following paragraphs.

[61] IDABC Decision 2004.

[62] See in particular Article 29 IMI Article 29 2007b, pp. 8, 10 and EDPS 2007, considerations 12–28.

[63] Article 29 IMI 2007, p. 10.

[64] European Commission 2007b, L13/18-23.

reservations as to the presence of a sufficient legal basis, particularly in relation to the requirements that such legal basis must be sufficiently clear and specific, and provide a sufficient degree of legal certainty.[65]

As we are now in fact confronted with the development of one of the first PEGS, it is all the more important that the requirements of legal certainty are met, as the path which is chosen now will undoubtedly have ramifications toward the approaches that will be taken in the future. Currently, it is still uncertain whether the current bases shall be found sufficient, or whether additional regulatory action would be taken. The EDPS and the Commission have in this regard agreed to follow a "step-by-step" approach, in which Recommendation 2009/329/EC is the first important step.[66]

For purposes of completeness, we note that none of these instruments make reference to use of consent as a legitimacy ground.[67]

15.3.1.3 Data Quality

We earlier characterized the IMI System as a "federation of Authoritative Sources" (cf., *supra*, Sect. 15.3.1). Data accuracy is thus primarily achieved by directing users of the system to the entity which is trusted to provide reliable and up-to-date information. However, Recommendation 2009/329/EC currently does not provide any additional guidelines or baseline requirements as to how participating Member States should maintain the accuracy of the information.[68]

As far as the retention period is concerned, Article 4 of Decision 2008/49/EC provides that personal data relating to data subjects, which are not IMI users themselves, shall be erased 6 months "after the formal closure of an information exchange, unless erasure before that period is expressly requested by a competent

---

[65] EDPS 2007, considerations 18 et seq. See also Sect. 15.2.1.

[66] See recital 8 of European Commission 2009, as well as the correspondence between the EDPS and the Commission, available at http://ec.europa.eu/internal_market/imi-net/data_protection_en.html.

[67] Seeing as verification through IMI may in fact be a prerequisite toward exercise of a professional activity in a particular Member State, consent would not provide an appropriate basis for the processing as the data subject's consent would arguably not be "freely given" (see Art. 2, h DPD). Cf., Sect. 15.2.1.

[68] This may be attributed to the fact that the respective databases are also governed by national data protection regulations, which already require this information to be accurate. Nevertheless, we consider it recommendable that some baseline requirements or, alternatively additional guidance (e.g., in the form of "best practices"), be issued as to the procedures participating Member States are expected/recommended to maintain in order to ensure data accuracy. See also FIDIS D16.3, 2009c, p. 19. We do note, however, that under Section 13 —"Work in progress" of European Commission 2009, reference is made to the creation of an online procedure which would, *inter alia*, enable rectification of inaccurate data.

authority to the Commission".[69] The EDPS has questioned whether there is in fact a legitimate reason to keep the data in IMI for another 6 months after the formal closure of an information exchange.[70] It recommends that, rather than from the date of "formal closure", the 6 months deadline for automatic deletion should start as of the date when the requesting authority first contacts its counterpart in any specific information exchange (in other words, counting the deadlines from the start of an exchange).[71]

In order to help ensure the proportionality (and transparency) of processing, the Commission has published sets of pre-defined questions and pre-defined data fields corresponding to a particular data exchange. The EDPS has not only applauded this good practice, but also recommended that a legal instrument should be adopted to provide an obligation for the Commission to do so.[72] In addition, the EDPS also made the following recommendations regarding proportionality.[73]

- A clear specification that IMI is not intended to be routinely used to do background checks on migrant professionals and service providers, but only in case applicable legislation allows it and where there are reasonable doubts as to (i) the authenticity of the information provided by the migrant service provider to the Competent Authority in the host Member State or (ii) his/her eligibility to establishment or exercise of his/her profession in the host Member State.
- In order to minimize unnecessary transmission of sensitive but not always relevant data, a provision laying down that whenever no actual criminal record information is strictly necessary to be transferred, pre-defined questions and answers in the IMI interface should not include a request for criminal records and should be phrased differently, in such a way to minimize sharing sensitive data.

The Commission has included statements that reflect these considerations in Recommendation 2009/329/EC.[74]

15.3.1.4 Transparency and Accommodation of Data Subject Rights

As far as the accommodation of data subject rights (notice, access, rectification, erasure, and blocking) is concerned, Commission Decision 2008/49/EC provided that[75]

---

[69] European Commission 2007b, L13/18-23. Note that the retention period toward personal data of IMI users is governed by Art. 5 of 2008/49/EC rather than Art. 4.

[70] EDPS 2007, consideration 41.

[71] Ibid., consideration 41.

[72] Ibid., considerations 31–32.

[73] Ibid., consideration 33.

[74] See in particular Section 8 of European Commission 2009.

[75] Art. 3 of European Commission 2007b.

> The controllers shall ensure that the data subject may effectively exercise its rights to information, to access, to rectify, and to object according to the applicable data protection legislation. The IMI actors shall provide privacy statements in an appropriate form.

Seeing as the definition of the respective roles in Article 3 was not extremely detailed (cf., *supra*, Sect. 15.3.1.1), this clause did not provide much clarification as to how the accommodation of data subject rights should be organized. With regard to the notice requirements, the EDPS recommended the adoption of several additional paragraphs to address this issue, following a "layered approach.[76] First, the EDPS recommended that the Commission adopt a comprehensive privacy notice on its IMI webpage, including all the items required under Articles 10 and 11 of Regulation EC No. 45/2001.[77] Said notice should not only cover the processing operations performed by the Commission, but should also include a general notice with regard to the information exchanges between Competent Authorities. Secondly, it recommended that each Competent Authority provide a privacy notice on its own webpage, which cross-references the notice provided by the Commission, together with further details specific to that particular authority or Member State. Finally, the data subjects should also, at the latest of the time of uploading of personal data relating to them, be given notice directly (except where an exemption to the notification obligation is applicable).

With regard to the data subject rights of access, objection, and rectification the EDPS recommended that an additional paragraph be adopted which[78]

- Specifies to whom data subjects should address their access request, objection, or request for rectification.
- Specifies which Competent Authority will be competent to decide about those requests.
- Sets forth a procedure in case the data subject submits his/her request to an IMI actor which is not competent in deciding about those requests.[79]

Commission Recommendation 2009/329 does include a privacy statement, which has also been published on the Commission IMI website. The same recommendation also provides a number of suggestions with regard to how competent authorities could (or should) comply with their notice obligations.[80] The Commission has also outlined how requests for rectification and the exercise of the right of access should be accommodated. In order to reduce the burden on the data subjects involved (who are unlikely to be familiar with the technicalities of the

---

[76] See EDPS 2007, considerations 36–38.

[77] Regulation No. 45/2001/EC, L8/1-22. As indicated earlier, we have not referred separately to the provisions of this regulation throughout this document, seeing as all of the provisions relevant to our analysis here, are almost identical to the corresponding provisions in Directive 95/46/EC.

[78] EDPS 2007, consideration 37.

[79] The EDPS also added that it should be specified that the Commission can only provide access to data to which it itself has legitimate access—see consideration 38.

[80] See European Commission 2009, Section 9.

joint-controller and joint-processing operations performed within IMI), Recommendation 2009/329 provides that

> No competent authority should refuse access, rectification or deletion on the ground that it did not introduce the data in the system or that the data subject should contact another competent authority. The competent authority receiving the request will examine it and grant or refuse it in accordance with the merits of the request and the provisions of its own national data protection law. If necessary and appropriate, the competent authority may contact other competent authorities before taking a decision.[81]

This particular guideline of course does not yet deal with the complications that may arise when the data in question has in fact already been communicated to another competent authority. Article 12, c of Directive 95/46/EC requires the controller to notify any rectification, erasure, or blocking to third parties to whom the data has been disclosed, unless this proves impossible or involves a disproportionate effort. To address this requirement, the Commission has announced it is working on a feature within the IMI system that would allow online data rectifications and support automatic notifications to those competent authorities involved.[82]

15.3.1.5 ID Number Policy

A final aspect of data protection important to this case study is the use of identification numbers within IMI. Initially, the Commission advanced the viewpoint that national restrictions on the exchange of unique identifiers "would not [be] justified" because the use of data would "certainly make the exchange between competent authorities easier".

In Opinion 07/2007, the Article 29 Working Party emphasized the sensitivity of this question. In particular, it pointed to the discretion of the Member States in this regard pursuant to Article 8.7 of Directive 95/46/EC (Article 29 IMI Article 29 2007b, pp. 15–16). It reminded the Commission that the Member States shall be competent to determine all the conditions and modalities under which a national identification number may be conveyed via IMI, including possible restrictions such as the requirement of authorization by dedicated committees set up within national data protection authorities (Article 29 IMI Article 29 2007b, p. 16). It did not, however, adopt a normative statement with regard to the need or appropriateness of using national identification numbers in the context of IMI. Rather, it emphasized only the deference which needs to be given to Member States in this regard pursuant to Directive 95/46/EC.

---

[81] European Commission 2009, in particular pp. 25–26.

[82] See European Commission 2009, in particular p. 26. Until this feature has become operational, the Commission expects competent authorities to address such requests for rectification directly to the IMI data controller at the European Commission (as identified in the IMI Privacy Statement).

In its 2009 Recommendation, the Commission introduced the following provision.

> The requesting competent authority should provide only the personal data that the responding competent authority needs to be able to unambiguously identify the person in question or to answer the questions. For example, if a migrant professional can be identified by his name and registration number in a professional registry, there should be no need to also provide his personal identification number (European Commission 2009, p. 20).

We are pleased to see that the Commission has adopted the view that the use of national ID numbers must at least be proportionate, by advocating the use of "least intrusive" means as far as identification of the data subjects is concerned. While from a privacy perspective, the suggested approach is naturally preferred to the propagation and use national identifiers of more general application; at the same time it lacks any reference to future integration of more privacy-enhancing approaches, nor does it address what the impact of this approach may be in the long term. We have indicated earlier that it is not the purpose of this chapter to detail the possible alternative models with regard to the use of national identifiers in the context of PEGS. This aspect of the development of the IMI system does, however, illustrate the need for further reflection and debate with regard to the usage of identifiers within PEGS.[83]

15.3.2 The Increasing Use of Biometric Data

Biometric data is increasingly used for e-government purposes in various applications in the European Union. The reason is that biometric references facilitate the identification or the verification of the identity of persons in an automated way. The biometric data is often stored in centralized databases. One of the first large-scale information systems relying upon biometric data is Eurodac, which was set up with the aim of improving border control and immigration management. The use of biometric data is also expanding to other types of applications such as VIS and SIS II. In certain instances, we have also witnessed the repurposing of the information that is processed in these systems. In the following subsection we shall provide a brief overview of some of these databases and applications. Thereafter, it will be reviewed whether and how the privacy and data protection principles we have selected, have been taken into account in the development of these applications.

15.3.2.1 Large-Scale Biometric Applications: Some Examples

Eurodac. In 2000, the EU central fingerprint database Eurodac (European Dactylographic System) was created. Eurodac helps to determine which EU Member

[83] Cf., Sect. 15.2.7.

State is responsible for examining the asylum application lodged by a third-country national in one of the Member States pursuant to the Dublin Convention.[84] The system was intended to speed up asylum procedures and to detect double requests among the asylum-seekers' applications that were lodged with different EU Member States. Eurodac became operational in 2003. It enables identification of asylum-seekers, as well as cross-checking of fingerprints of asylum seekers and aliens apprehended in connection with irregular crossing of an external border or found illegally present in a Member State. Eurodac was established as an instrument in the first pillar.[85] Data such as the Member State of origin, fingerprints, sex, and the reference number used by the Member State of origin are recorded. In the event that a fingerprint comparison provides positive results, additional data such as name, picture, etc. is exchanged. Eurodac operates using the Automated Fingerprint Identification System (AFIS).

VIS. Not long after Eurodac, the EU Council of Ministers decided to establish the Visa Information System (VIS) (VIS Decision 2004). VIS is an information system intended to enable national authorities to enter and update visa data of third-country nationals and to consult these data electronically. Personal data recorded in the central database of VIS include not only a list of alphanumeric data, such as surname and first name, but also photographs and fingerprint data.[86] Access to VIS for identification purposes ("one to many check") whereby biometric data is used as a search criterion is expressly foreseen in the VIS Regulation Decision 2008 (Art. 20). VIS will also enable competent asylum authorities to search on the basis of fingerprints of asylum seekers, thereby facilitating the identification and return of illegal immigrants pursuant to the "Dublin II Regulation" (EC) No. 343/2003 (Art. 21). In the long-term, it is expected that VIS will be one of the largest biometric databases in Europe. By decision of the Council of 23 June 2008, designated authorities of Member States and Europol have obtained access to VIS for purposes of the prevention, detection, and investigation of terrorist offenses and other serious criminal offenses.[87]

Regulation 2252/2004 requires Member States to include a facial image and fingerprints in the electronic storage medium of the passport and travel documents issued to EU citizens. After the technical specifications had been set, this obligation for the Member States took effect as of June 29, 2009. The Regulation does not require Member States to set up or maintain a central database for the purposes of issuing such, but does not forbid this either. This aspect of implementation was left to the Member States. The Regulation further states that the biometric data

[84] See Dublin Convention 1997, Regulation 2725/2000/EC and Regulation 407/2002/EC. About Eurodac in general, see also Broeders 2009, pp. 48–51.

[85] There are three policy areas.

[86] Art. 5,1 of the Regulation 767/2008/EC.

[87] Decision 2008/633/JHA, p. 129.

shall only be used for "verifying the authenticity of the document and the identity of the holder when the passport or travel document is required to be produced by law." In the meantime, several Member States (e.g., France, the Netherlands)[88] have passed national legislation concerning which provides for the central storage of the collected biometric data. In some cases, express provisions are made for access to or use of this biometric data for specific investigations or by law enforcement authorities under specific conditions.[89]

15.3.2.2 Legitimacy of the Processing

As elaborated earlier, all processing of personal data by governments must be based on a clear and specific legal basis, pursue a legitimate aim and be proportionate with the aim that is pursued. The collection and storage of biometric data in central databases is problematic because it brings about specific risks for the privacy of the data subjects concerned.[90] In first instance, the central storage of biometric data is a key enabler for the performance of "one to many" identification checks. Additionally, central storage considerably increases the risks that the data might be used in a covert way (e.g., for tracing and tracking), or for purposes other than those initially intended.[91]

The legitimacy and legality of the central storage of biometric data has been questioned in several instances, e.g. in VIS. The VIS system was designed to provide border guards with all the information necessary to determine whether third-country nationals satisfy entry conditions. The Article 29 Data Protection Working Party expressed its concerns, wondering in particular what studies revealed compelling reasons of public safety or public order that would justify the central storage of biometric data and whether alternative approaches which do not involve such risks have been studied (Article 29 VIS 2004, pp. 4–5). In opinion also related to VIS, it stated that an

> Of the principle of proportionality therefore begs the question of the fundamental legitimacy of collecting these data. Extremely careful analysis of the lawfulness of the processing of such data for identification purposes is necessary, given the possible prejudicial effects to the persons concerned if they are lost or used for purposes other than those for which they were (Article 29 VIS 2005, p. 12).

---

[88] See also FIDIS D13.4, 2009b.

[89] This was for example, the case in the Netherlands. See Art. 4b, 2 and 4 of the Act of September 26, 1991 containing rules for the issuance of travel documents, as modified, available at http://www.st-ab.nl/wetten/1002_Paspoortwet.htm

[90] See and compare with a decision of the European Court of Human Rights in which the collection and central storage of DNA and biometric data was reviewed: ECHR Marper 2008.

[91] See also Kindt and Dumortier 2008, pp. 192 et seq.

Some also consider the extension of some of the large-scale processing systems to the police and Europol for security purposes, to be problematic and without basis in the EU Treaty.[92]

Last, but not least, the legitimacy of Regulation 2252/2004 which introduced the ePassport with two biometric identifiers has been heavily criticized.[93] Particular reference is made to Article 18(3) of the consolidated version of the Treaty Establishing the European Community, which excludes regulatory actions by Council in the field of passports, identity cards, and residence permits to facilitate the free movement of persons from the EU.

15.3.2.3 Re-purposing of Biometric Data

Until recently, the government typically only collected data relating to certain human characteristics from suspects and criminals for law enforcement purposes. Law enforcement operations are governed by specific legal principles (e.g., presumption of innocence, right to a fair trail, etc.) and are subject to strict conditions. However, the same data, for example fingerprints, are now widely collected from most citizens (e.g., when applying for an ePassport) and stored or used for applications outside of the area of law enforcement. It is expected that these applications will sooner or later also be used for different purposes ("function creep"). The French DPA (CNIL) for example, has already pointed out at various occasions that fingerprints were in the past mainly used by the police. Therefore, a database with fingerprints is likely to be used in the future by the police as well, and to effectively become "a new instrument of the police", notwithstanding the original purposes of the processing.[94]

The evolution of various large-scale databases, such as Eurodac and VIS, seems to confirm the fears of the CNIL. Eurodac, for example, has already seen proposals to extend the use and purposes of its database, which was originally intended as a mechanism for determining responsibility for asylum applications and as a database only accessible to asylum authorities. According to these proposals, the use of the database would be extended to basically all matters relating to law enforcement and public security in the EU, including terrorism.[95] In case of VIS, Regulation 2008/633/JHA[96] enables Europol and certain other authorities to access VIS for purposes of the prevention, detection, and investigation of terrorist offenses, as well as other serious criminal offenses. It has been questioned whether these

---

[92] See, for example, a Dutch group of experts on refugee law, presided by Mr. Meijers ("Meijers Committee") which strongly objects to the extension of Eurodac, available at http://www.commissie-meijers.nl/commissiemeijers/pagina.asp?pagkey=37264

[93] See De Hert and Schreurs 2006, pp. 60–62.

[94] See, e.g., CNIL 2000, p. 108.

[95] See Council of the European Union 2007. The EU Commission repeated the proposal in European Commission 2009.

[96] Decision 2008/633/JHA, pp. 129–136.

finalities and this form of access by these authorities is compatible with the original purposes and finalities of these large-scale databases.[97]

A significant factor in this evolution has been the articulation of the principle of availability. This principle was elaborated in the aftermath of September 11, 2001 and is aimed at providing national law enforcement agencies within the EU, full access to all the data in national and European databases. This principle was embedded in the "The Hague Program" which was adopted by the European Council in November 2004.[98] The "The Hague Program" also introduced the idea of the use of biometric identifiers for passports, visa information system, and interoperability of data systems in the EU.

As stated above, the current data protection framework does allow for re-purposing of collected data, provided the necessary compliance steps are taken (cf., *supra*, Sect. 15.2.2). However, when legislators decide to introduce biometric databases, they should take into account that later policies and decisions in the field of Freedom, Security, and Justice can transform these databases into instruments for use for a different purpose. This is not just a mere hypothesis, but actually happens, as illustrated above. Moreover, it should be noted that once particular data processing activities of governments fall within the remit of the second (in part) and third pillars, in particular the processing of data for security and law enforcement purposes, such processing is excluded from the scope of Directive 95/46/EC. At presently, there is not yet a comprehensive legal framework for the processing of personal data in these areas of security and law enforcement.

15.3.2.4 Data Quality

As elaborated above, personal data collected by governments must be accurate. Where biometric data is involved, data quality is of the utmost importance. Biometric data must be of a sufficient quality in order to be useful and relevant for automated comparison purposes. Where the collected samples prove to be inadequate to achieve the purposes for which they were collected, they should be deleted.

Some of the aforementioned databases have demonstrated that a considerable amount of biometric data collected by governments does not provide a sufficient level of data accuracy. For example, in the evaluation of the Dublin system, the EU Commission expressed concerns about the collection and the quality of data

[97] See, for example, the Meijers Committee, Intended legislation to amend Eurodac regulation would be unlawful and this risk to be annulled by the Court of Justice, 6 November Council of the European Union 2007, available at http://www.commissie-meijers.nl/commissiemeijers/pagina.asp?pagkey=37264 (accessed September 25 , 2009); FIDIS D3.6 Article 29 2007a, pp. 63–66.

[98] The adoption of the programme was followed by a 5 year programme presented by the EU Commission which set the objectives for the next 5 years for developing an area of Freedom, Security, and Justice.

sent to the Central Unit of Eurodac.[99] Statistics revealed that 6% of the data is rejected because of its low quality. Problems of data quality were similarly revealed in relation to the ePassports during some of the pilots conducted after the adoption of Regulation 2252/2004.[100]

15.3.2.5 The Risks of Biometric Identifiers

A biometric identifier is any biometric reference, such as a face image or fingerprint minutiae template, which can be used for the automated identification or verification of the identity of persons. Because biometric characteristics are often unique, they can usually be used as identifiers, which enable linkage and aggregation of information across various databases. This facilitates use of the data for other than the initially envisaged purposes, the creation of personal profiles, as well as the tracking and tracing of data subjects. The large-scale biometric systems discussed above also demonstrate that, because of these risks related to their usage, biometric identifiers were initially only introduced for non-EU nationals in the context of border management. Nevertheless, usage of biometric identifiers is gradually extending and has meanwhile also been introduced for EU citizens.[101]

As elaborated earlier, each Member State is to determine the conditions under which an identifier of general application may be processed. Few Member States, however, have adopted specific legislative measures to regulate use of biometric identifiers. France is a notable exception to this statement: since 2004, the French Data Protection Act[102] requires that the processing of biometric data by the government for the "authentication or the identity control" is authorized by a decree ("décret en Conseil d'Etat") in execution of the law. The CNIL has to render first its (non-binding) opinion which shall be public and motivated (Art. 27, I, 2°).

15.3.2.6 Security Flaws

The use of biometric characteristics in the systems and applications mentioned earlier often failed to incorporate the organizational and technical security measures which are needed to protect the rights of the data subjects. For example, the

[99] See European Commission 2007a, p. 9.

[100] Some of these quality problems have been expressly recognized in the EC Regulation 444/2009 amending EC Regulation 2252/2004. See recital (3): "During pilot projects in some Member States, it appeared that the fingerprints of children under the age of 6 seemed not to be of a sufficient quality for one-to-one verification of identity." Other quality problems relating to the face recognition were revealed during tests in Germany. See Bundeskriminalamt 2007.

[101] For example, every EU citizen who applies for a passport has to provide from now on, also his or her fingerprints, in addition to a digital facial image.

[102] Act No. 78-17.

ePassports make use of an RFID medium for the storage of biometric characteristics. However, an unprotected ePassport RFID chip is subject to short-range clandestine scanning up to some feet and allows for the illegal listening into an existing communication (eavesdropping), with leakage of personal information.[103] Because of the lack of a convincing security concept for ePassports, the FIDIS research group called for immediate action and implementation of organizational and technical procedures to protect the information stored, especially the biometric data.[104]

15.4 Conclusion

The current legal framework does not offer ready-to-use answers to the questions which arise in respect of e-government identity management. Recurring issues relate to the legitimacy of processing, the determination of roles and responsibilities, the re-purposing of personal data, and the transparency of processing. Another ongoing challenge lies in the development of appropriate information security and governance frameworks that ensure an adequate level of assurance and protection for every aspect of the processing. An area which might particularly benefit from further research and debate is the usage of identifiers in Pan-European e-government services.

The case studies described in this chapter illustrate that e-government initiatives taken at the European level are not always exemplary in addressing privacy concerns. During the development of the Internal Market Information system the European Commission has, in dialogue with the Article 29 Working Party and the EDPS, taken very important steps towards ensuring the privacy-friendly development of PEGS. While certain initiatives show great promise (e.g., with regard to accommodation of data subject rights), there are still areas in which a comprehensive approach is still missing (e.g., data accuracy, ID number policy). The current practices in the area of demonstrate that often design decisions are still mainly driven more by considerations of efficiency and use rather than the protection of citizens' privacy interests. The increased deployment of biometric information systems and the continued propensity towards central storage raises concerns due to the specific risks this approach entails. These concerns are augmented by the absence, in most Member States, of a dedicated regulatory framework which determines specific conditions under which biometric identifiers may be processed.

[103] See also Juels et al. 2005 and FIDIS D3.6, 2007a, p. 117.

[104] FIDIS 2006.

References

Article 29 eGov (2003) Article 29 Data Protection Working Party, Working document on e-government, WP 73. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_en.pdf. Accessed 8 May 2003

Article 29 VIS (2004) Article 29 Data Protection Working Party, Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS), WP 96, 11 Aug 2004

Article 29 EHR (2007) Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf. Accessed 15 Feb 2007

Article 29 IMI (2007) Article 29 Data Protection Working Party, Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI), WP140, published online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp140_en.pdf. Accessed 20 Sept 2007

Article 29 VIS (2005) Article 29 Data Protection Working Party, Opinion 2/2005 on the proposal for a regulation of the European parliament and of the council concerning the visa information system (VIS) and the exchange of data between Member States on short stay-visas, WP 110, 23 June 2005

Belgian DPA (2008) Commission for the protection of privacy, aanbeveling 01/2008 met betrekking tot het toegangs–en gebruikersbeheer in de overheidssector recommendation nr. 01/2008 of 24 Sept 2008 concerning user- and access management in the governmental sector. 24 Sept 2008. http://www.privacycommission.be/nl/docs/Commission/2008/aanbeveling_01_2008.pdf

Belgian DPA reference measures commission for the protection of privacy, referentiemaatregelen voor de beveiliging van elke verwerking van persoongegevens (reference measures for the security of every type of personal data processing). http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

Broeders D (2009) Mobiliteit en surveillance: een migratiemachine in de maak. In: Dijstelbloem H, Meijer A (eds) De migratiemachine serie kennis openbare mening, politiek. Rathenau Instituut/Van Gennep, Amsterdam, pp 35–59

Bundeskriminalamt (2007) Forschungsprojekt. Gesichtserkennung als fahndungshilfsmittel foto-fahndung. Abschlussbericht, Wiesbaden, Feb 2007

Bygrave LA (2001) Core principles of data protection. Privacy law and policy reporter 7 (9). http://www.austlii.edu.au/au/journals/PLPR/2001/9.html

CNIL (2000) 21e rapport d'activité 2000. www.cnil.fr

Council of the European union (2007) Council conclusions on access to Eurodac by member states' police and law enforcement authorities as well as Europol, Luxembourg, 12 and 13 June 2007, 2807th meeting JHA council, of which a draft is available at http://register.consilium.europa.eu/pdf/en/07/st10/ st10002.en07.pdf

De Bot D (2001) Verwerking van persoonsgegevens (processing of personal data). Kluwer, Antwerpen

De Bot D (2005) Privacybescherming bij e-government in België. Een kritische analyse van het rijksregister, de kruispuntbank van ondernemingen en de elektronische identiteitskaart (privacy protection in e-government in Belgium. A critical analysis of the national register, the crossroadsbank for enterprises and the electronic identity card). Vandenbroele, Brugge

Decision 2008/633/JHA Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the visa information system (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 13.08.2008, L 218/129-136

Deprest J, Robben F (2003) E-government: the approach of the Belgian federal administration. https://www.law.kuleuven.be/icri/frobben/publications/2003%20-%20E-government%20paper%20v%201.0.pdf

ECHR Marper (2008) European court of human rights, S. and Marper v. U.K., GC, Nos. 30562/04 and 30566/04, 4 Dec 2008

EDPS (European Data Protection Supervisor) (2007) Opinion on the commission decision of 12 Dec 2007 concerning the implementation of the internal market information system (IMI) as regards the protection of personal data (2008/49/EC). OJ 25.10.2008, C 270/1-7

EPIC (Electronic Privacy Information Center and Privacy International) (2007) Privacy and human rights 2006. An international survey of privacy laws and developments, 2007, p 25

European Commission (2003) Communication from the commission to the council, the European parliament, the European economic and social committee and the committee of the regions, 'the role of e-government for Europe's future', SEC (2003) 1038, COM (2003) 567 final, 26 Sept 2003, p 26. http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf

European Commission (2005) Information society and media directorate-general, e-government unit, 'a roadmap for a pan-European eIDM framework by 2010', vo1 0, p 20. http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf

European Commission (2007a) Report from the commission to the European parliament and the council on the evaluation of the dublin system, COM (2007) 299 final, 6.06.2007, p 13. http://ec.europa.eu/justice_home/news/intro/doc/com_2007_299_en.pdf

European Commission (2007b) Commission decision 2008/49/EC of 12 Dec 2007 concerning the implementation of the internal market information system (IMI) as regards the protection of personal data. OJ 16.01.2008, L 13/18-23

European Commission (2009) Commission recommendation 2009/329/EC of 26 March 2009 on data protection guidelines for the internal market information system (IMI). OJ 18.04.2009, L 100/12-28

FIDIS (2006) Budapest declaration on machine readable travel documents (MRTDs). Frankfurt. www.fidis.net

FIDIS D3.6 (2007a) Meints M, Hansen M (eds) D.3.6 Study on ID documents, FIDIS, 2006. www.fidis.net

FIDIS D13.3 (2007b) Buitelaar JC (ed) D13.3 Study on ID number policies. FIDIS deliverable, 2007. www.fidis.net

FIDIS D16.1 (2008) Buitelaar JC, Meints M, Van Alsenoy B, D16.1 Conceptual framework for identity management in e-government. FIDIS deliverable, 2008. www.fidis.net

FIDIS D3.17 (2009a) Meints M, Zwingelberg H (eds) D3.17 Identity management systems—recent developments. FIDIS deliverable, 2009. www.fidis.net

FIDIS D13.4 (2009b) Kindt E, Müller L (eds) D13.4 The privacy legal framework for biometrics. FIDIS, May 2009. www.fidis.net

FIDIS D16.3 (2009c) Buitelaar JC, Meints M, Kindt E (eds) D16.3 Requirements for identity management in e-government. FIDIS deliverable, 2009. www.fidis.net

Hert P De, Schreurs W (2006) Legal grounds for ID documents in Europe (sections 4.1.1–4.1.5). In: Meints M, Hansen M (eds) D.3.6 Study on ID documents. FIDIS, pp 40–70

Hulsebosch B et al (2009) D2.3 Quality authenticator scheme. STORK deliverable. http://www.eid-stork.eu

Huysmans X, Van Alsenoy B (eds) (2007) D1.3 Conceptual framework—annex I. Glossary of terms, IDEM, vo1. 0.7. https://projects.ibbt.be/idem/uploads/media/2007-12-27.idem.glossary.v1.07.pdf

IDABC (2007) Graux H, Majava J (2007) eID interoperability for PEGS. Analysis and assessment of similarities and differences—impact on eID interoperability. IDABC, Nov 2007. http://ec.europa.eu/idabc/servlets/Doc?id=29618

IDABC Decision (2004) Decision 2004/387/EC of the European parliament and of the council of 21 April 2004 on the interoperable delivery of pan-European e-government services to public

administrations, businesses and citizens (IDABC). OJ 30.04.2004, L 144, as corrected by OJ 18.05.2004 L 181/25-35

ITU-T (2007) International telecommunication union—telecommunication standardization sector. Focus group on identity management, report on identity management framework for global interoperability. http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

Juels A, Molnar D, Wagner D (2005) Security and privacy issues in e-passports. Sept 2005. http://eprint.iacr.org/cgi-bin/print.pl

Kindt E, Dumortier J (2008) Biometrie als Herkenning—of Identificatiemiddel? Enkele juridische beschouwingen. Computerrecht 132:185–198

Kosta E, Dumortier J (2007) The data retention directive and the principles of European data protection legislation. Medien Recht Int 3:130–136

Leenes R et al (2009) D2.2 Report on legal interoperability. STORK deliverable. http://www.eid-stork.eu

Léonard Th (2004) La protection des données à caractère personnel et l'entreprise (the protection of personal data and the enterprise). In: Guide juridique de l'entreprise (legal guide for the enterprise). Brussels, Kluwer, Livre 112.1, pp 9–64

McCallister E, Grance T, Scarfone K (2009) Guide to protecting the confidentiality of personally identifiable information (PII). Special publication 800-122, NIST. Draft version available at http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf

Menezes AJ, Van Oorschot PC, Vanstone SA (1997) Handbook of applied cryptography. CRC Press, Boca Raton

Millard J (ed) (2007) European eGovernment 2005–2007: taking stock of good practice and progress towards implementation of the i2010 e-government action plan. Sept 2007, p 82. http://www.epractice.eu/files/download/awards/ResearchReport2007.pdf

Modinis (2006) Modinis study on identity management in eGovernment, modinisIDM. A conceptual framework for European IDM systems. Modinis project, 18 Sept 2006. http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_conceptual_framework.pdf

Modinis (2007) Modinis study, breaking barriers to e-government—deliverable 3: solutions for eGovernment (section 1). 2007, p 82. http://www.egovbarriers.org/downloads/deliverables/solutions_report/Solutions_for_eGovernment.pdf

Papakonstantinou V (2001) A data protection approach to data matching operations among public bodies. Int J Law Inf Technol 9(1):39–64

Roessler T (2002) Identification and authentication in networks enabling single sign-on. Master thesis, Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria, 2002. https://online.tugraz.ac.at/tug_online/voe_main2.getvolltext?pDocumentNr=84179

Schreurs W, De Hert P (2005) Vragen over privacy bij biometrisch paspoort en elektronische identiteitskaart (privacy questions with regards to the biometric passport and the electronic identity card). Juristenkrant 104, pp 6–10

Van Alsenoy B, De Cock D (2008) Due processing of personal data in e-government? A case study of the Belgian electronic identity card. Datenschutz und Datensicherheit, March 2008, pp 178–183. http://www.fidis.net/fileadmin/fidis/publications/2008/DuD-2008-03-Due-processing-of-personal-data-in-eGovernment.pdf

Van Alsenoy B et al (2009) Delegation and digital mandates: legal requirements and security objectives. CLSR 25:415–431

VIS Decision (2004) Council decision of 8 June 2004 establishing the visa information system (VIS), 2004/512/EC. OJ 15.06.2004, L 213/5-7

Chapter 16
eHealth from a Dutch Perspective

Hilde van der Meer and Sjaak Nouwt

Abbreviations

BIG Act	Wet Beroepen in de individuele gezondheidszorg (Individual Healthcare Act)
CVZ	College voor Zorgverzekeringen (Health Care Insurance Board)
EHR	Electronic Health Record
EPD	Elektronisch Patienten Dossier (Electronic Health Record)
epSOS	Smart Open Services for European Patients
GP	General Practitioner
I.COM	Innovation Centre of Mental Health and Technology
ICT	Information and Communication Technologies
IGZ	Health Care Inspectorate
Kwz	Kwaliteitswet zorginstellingen (Quality of Healthcare Institutions Act)
LMI	Lead Market Initiative
LSP	National Switch Point
NVEH	De Nederlandse Vereniging voor e-Health (Dutch Association of eHealth)
NZa	Dutch Healthcare Authority
RVZ	Council for Public Health and Health Care
SGEI	Services of General Economic Interest

Contribution received in 2010.

H. van der Meer · S. Nouwt (✉)
Royal Dutch Medical Association (KNMG), Utrecht, The Netherlands
e-mail: s.nouwt@fed.knmg.nl

H. van der Meer
e-mail: h.vd.meer@fed.knmg.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*,
Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_16,

TCCN	Stichting Teledermatologisch Consultatie Centrum (Teledermatological Consultation Centre Netherlands)
WGBO	Wet geneeskundige behandelingsovereenkomst (Medical Treatment Contract Act)
WVP	Wet Bescherming Persoonsgegevens (Personal Data Protection Act)
ZVW	Zorgverzekeringswet (Health Care Insurance Act)

Contents

16.1 Introduction 284
16.2 Developments Related to eHealth 285
16.2.1 Introduction 285
16.2.2 European Policy Developments 286
16.2.3 eHealth Developments in the Netherlands 289
16.3 The European Legal Framework for eHealth 294
16.3.1 Introduction 294
16.3.2 The European Legal Framework 295
16.4 A Dutch Analysis of the European Legal Issues 305
16.4.1 Introduction 305
16.4.2 Patient Data Protection, Privacy, and Confidentiality 306
16.4.3 Product, Services, and Professional Liabilities 308
16.4.4 Competition Law 309
16.4.5 Patient Safety and Quality of Care 310
16.5 Conclusion 311
References 312

16.1 Introduction

In this chapter, we will focus on the legal issues that relate to the eHealth developments in Europe and in the Netherlands. We will analyze these legal issues after setting out the European legal framework for eHealth. But before that, we will describe the eHealth policy developments at the EU level and we will give a few examples of eHealth services in the Netherlands. Our conclusion will focus on the importance of eHealth services and of the legal framework for the quality of healthcare and the quality of life.

Before describing the developments in eHealth in Europe and in the Netherlands, we will first explain what is meant by eHealth. A very broad definition is given by the European Commission on their thematic portal about eHealth. The Commission defines eHealth as: 'Information and Communication Technologies Tools and Services for Health.'[1] Like the World Health Organization, the EU

[1] See http://ec.europa.eu/information_society/activities/health/whatis_ehealth/index_en.htm. Accessed 21 December 2009.

focuses on the tools and services and covers nearly every application of ICT in healthcare. Another definition, by the Dutch Association of eHealth (NVEH), focuses more on the primary healthcare process and the interaction between health professionals and health consumers: 'the use of innovative ICT to support or improve health and healthcare.'[2] This definition includes distance healthcare applications like telemedicine. It is our opinion that the use of eHealth applications should indeed be supportive to the healthcare process and should improve the quality and safety of healthcare.

Telemedicine is, again technically, defined by the European Commission as: 'the provision of healthcare services, through the use of ICT, in situations where the health professional and the patient (or two health professionals) are not in the same location. It involves secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment, and follow-up of patients.'[3] A number of services are covered by this definition of telemedicine, like teleradiology, telepathology, teledermatology, teleconsultation, telemonitoring, telesurgery, and teleopthalmology. Other potential services are call centers or online information centers for patients, remote consultation and e-visits, or videoconferences between health professionals.

Health information portals, electronic health record systems, electronic transmission of referrals (e-prescription, e-referrals) are not telemedicine services. However, these services do fall within the concept of eHealth, and therefore, when appropriate, we will also refer to services like these.

16.2 Developments Related to eHealth

16.2.1 Introduction

The further development and use of eHealth is an important objective of EU policymaking. In this section we will shortly describe recent EU policy developments up until December 2009. Under the influence of both EU and national policymakers, in the Netherlands, eHealth tools are developed and becoming an integrated part of healthcare. In the second part of this section we will give a few examples of eHealth applications in the Netherlands.

---

[2] Seehttp://www.nveh.nl/index.php?option=com_content&view=article&id=67&Itemid=41. Accessed 21 December 2009.

[3] Commission of the European Communities 2008c.

16.2.2 European Policy Developments

16.2.2.1 eHealth Action Plan

In 2004, the European Commission published the eHealth Acton Plan.[4] The purpose of this Action Plan is to stimulate the development and use of eHealth systems.

As a result of the eHealth Action Plan, the Member States have drawn up national and regional roadmaps for eHealth, defined a common approach to patient identifiers, outlined interoperability standards for health records, and health data messages, and supported investments in eHealth.[5]

16.2.2.2 i2010

eHealth is an integrated topic in the EU's i2010 policy framework. The purpose of this framework is to promote the positive contribution that ICT can make to the economy, society, and personal quality of life.[6]

16.2.2.3 Lead Market Area

eHealth is also one of the six Lead Market Areas in the Lead Market Initiative (LMI) for Europe.[7] The aim of recognizing eHealth as a Lead Market Area is to develop a European market for innovative eHealth technologies and to combat fragmentation in the way healthcare is delivered in the different Member States.[8] The Action Plan of the Lead Market Initiative in the Area of eHealth, describes the European plans for implementation of ICT solutions for patients, medical services, and payment institutions.[9] The starting point in this action plan is that eHealth can help to deliver better care for less money within citizen-centered health-delivery systems. The assumption is that, over the past decades, investments in eHealth have stayed behind to those in other service sectors. Possible causes are the lack of

---

[4] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, and the Committee of the Regions, e-Health—making healthcare better for European citizens: An action plan for a European e-Health Area. Brussels, 30.04.2004. COM (2004) 356 final.

[5] European Commission 2008b.

[6] Source: http://ec.europa.eu/information_society/eeurope/i2010/strategy/index_en.htm. Accessed 20 July 2009.

[7] Source: http://ec.europa.eu/enterprise/policies/innovation/policy/lead-market-initiative/index_en.htm#h2-a-lead-market-initiative-for-europe. Accessed 20 July 2009.

[8] Commission of the European Communities 2008b.

[9] Commission of the European Communities 2007b.

Table 16.1

Objective	Action
Improve legal certainty and consumer confidence	Screen existing EU legislation related to eHealth and provide clarification and guidance for applying the legal framework for eHealth products and services
	Assess possibilities for adoption of a legal initiative for eHealth and telemedicine
	(Actions by EC)
Ensure protection of personal data in eHealth systems	Adopt an initiative to promote application and enforcement of Personal Data Protection legislation related to eHealth
	(Action by EC)
Enhance enforcement of consumer protection legislation by Member States for eHealth products	Promote knowledge and information dissemination on safe and secure eHealth products and use of existing infrastructure to protect consumers—networks, best practice repositories, hotlines
	(Action by EC)
Improve cross-border reimbursement	Introduce the Electronic Health Insurance Card
	Improve legal clarity regarding medical reimbursement based on recommendations from the Health Services Initiative
	(Actions by EC + Member States)
Support patient mobility	Provide citizens with relevant and up-to-date information on cross-border health services
	(Action by EC + Member States)

legal certainty for reimbursement, liability, and a lack of awareness on the correct application of data protection regulations. Apart from these legal causes, different social security systems and the lack of systems interoperability are also considered causes for the hindering of eHealth investments. According to the action plan, 'standardization, for instance, of various information exchange formats, certifications of interoperable systems, and large-scale demonstration projects (including the legal and organizational feasibility) could help to overcome this'.

With regard to the legal policy instruments, the action plan formulates objectives and actions to be taken between 2008 and 2010 (see Table 16.1).

In 2009, the Commission, in collaboration with the Member States, has committed to tackle a set of challenges related to legal and regulatory issues, which could hinder the development of eHealth.[10] These include, for example, new liability rules to cover eHealth products and services. Patients should also be given clear information concerning the costs of eHealth services. Healthcare organizations should make more use of eHealth to reduce accidents at the workplace and illnesses resulting from work.

[10] Source: http://ec.europa.eu/information_society/activities/health/policy/targets/index_en.htm. Accessed 20 July 2009.

16.2.2.4 Patient Safety

According to the i2010 Mid-Term Review (2008), eHealth plays a key role in the transformation of health care systems. Without eHealth, the costs of healthcare are expected to explode in the next decade, given the aging society and the increase in chronic diseases, with an increasing demand for better healthcare.

16.2.2.5 Interoperability of Health Records and Health Services (Patient Safety)

Already in the eHealth Action Plan (2004), the European Commission recognized the importance of interoperability of Electronic Health Record Systems. On 2 July 2008, the Commission issued the Recommendation on cross-border interoperability of electronic health record systems as a follow-up to the eHealth Action Plan, which, in 2004, defined interoperability of electronic health records as one of the priorities for Member States.[11]

The key objective of this recommendation is to provide patients with a choice to access information stored in electronic health record systems, regardless of place and time.

According to the Recommendation, the overall European eHealth interoperability should be achieved by the end the year 2015.

Interoperability is also a central issue in other projects. We limit ourselves by just pointing at two European projects on interoperability. The first one is epSOS: Smart Open Services for European Patients, which has two goals: the first goal is to establish a basic European Patient Summary to enable secure access for health professionals to the data of a patient from another country in their own language, using different technologies and systems.[12] The second goal is to facilitate electronic prescriptions across national borders. The epSOS project was launched on 1st of July 2008 with a duration of 36 months.

The second project is the Call for Interoperability (CALLIOPE) Thematic Network.[13] The CALLIOPE Network is a part of the Open eHealth Initiative, which is driven by the health administrations of the Member States. It's aim is to establish an appropriately governed, composed, and structured open forum to support Member States to implement interoperable eHealth solutions. The CALLIOPE Network was launched on 1st June 2008 with a duration of 30 months.

Recently, a collaboration project called CALLepSOS was introduced, linking CALLIOPE and epSOS.

---

[11] Commission of the European Communities 2008a.

[12] Source: epSOS 2008.

[13] Source: CALLIOPE 2009.

16.2.2.6 Prague Declaration

On 20 February 2009, at the eHealth 2009 Conference, the Member States and the European Commission adopted the Prague Declaration.[14] The Declaration encourages the Member States to take action on telemedicine, interoperability, and European cooperation including exchange of best practices. The Member States are encouraged to adapt their national eHealth strategies to make individuals (patients and healthcare professionals), society, and economy all benefit from eHealth's positive effects. The Member States are also urged to participate in discussions about a Europe-wide governance structure for eHealth. This should give additional impetus to the introduction of new services while removing existing obstacles.

16.2.2.7 eHealth on the Political Agenda of Sweden's Presidency

From 1 July to 31 December 2009, Sweden held the presidency of the EU. In July 2009, the Swedish Healthcare Division presented an Activity Plan on eHealth during the Swedish Presidency of the EU.[15]

The Swedish Presidency is of the opinion that eHealth must be accorded greater prominence on the political agenda, and a basis for structured cooperation must be established. According to the Swedish Presidency, policy makers, and healthcare providers should not only focus on effectiveness and efficiency, but also improve other political aspects of healthcare, such as Availability, Continuity of care, Empowerment, Patient safety, and Quality of care.

What is also important is that the Swedish Presidency wants eHealth to be perceived as an operational—as opposed to a technological—development issue. From this perspective, it is anxious to ensure that information about the concrete benefits of eHealth is disseminated. To demonstrate the connection between political goals, eHealth technologies, and potential benefits, the Swedish Presidency presented the report 'eHealth for a Healthier Europe' that was conducted on behalf of the Swedish Ministry of Health and Social Affairs. This report stresses, for example, the necessity for each Member State to prioritize eHealth initiatives based on political goals and documented benefits.

16.2.3 eHealth Developments in the Netherlands

In 2002, the Council for Public Health and Healthcare (RVZ) published the advisory report 'eHealth in sight.'[16] It was a follow up to the advisory report 'Patient and Internet' that the Council published in 2000.

---

[14] The Prague Declaration 2009.

[15] Swedish Presidency of the European Union, Healthcare Division 2009.

[16] The English summary of this advisory report is available at: http://www.rvz.net/cgi-bin/rvz_p.pl?id=68. Accessed 21 December 2009.

The report recognized that eHealth can contribute towards the realization of high-quality, accessible, and cost-effective healthcare. It was also analyzed that there are a number of barriers for the development of eHealth in the Netherlands. Electronic exchange of data between health professionals is not always possible, because data are not always recorded in electronic form and because of the lack of technical standards. Another barrier is the health professionals' fear for change: the existing culture is not open to new ICT tools, according to the RVZ. There are also financial and economic obstacles: e.g., the issue of reimbursement is unclear. Finally the legal barrier: privacy and security seem insufficiently secured.

In February 2005, the Dutch Association of eHealth (NVEH) was established.[17] The NVEH is the main association for eHealth and telemedicine in the Netherlands. The NVEH's main objective is to maintain and improve the quality of the eHealth product in the Netherlands. Other objectives of NVEH are to act as a point of mutual interest in eHealth for patient organizations, public authorities, advisory bodies, health insurance companies, health professionals, industry, research, education and trade organizations. And also to offer a platform for conference and consultation on eHealth matters and exchange knowledge, skills, and research outcomes.

On 24 June 2009, two health insurance companies (Achmea and Menzis), one bank (Rabobank), and one telecom provider (KPN) commisioned the Netherlands Organization for Applied Scientific Research TNO, to investigate how the spread and use of eHealth services in the Netherlands can be upgraded.[18] It appears that barriers for the development of eHealth services in The Netherlands are:

- Culture and social support of the health consumer
- Social support of health professionals
- The supply of services and know–how
- The lack of medical and economic scientific back up
- Unification and standardization
- Financing
- Laws and Regulations

These barriers are not new. They were also recognized by the Dutch Court of Audit ('Algemene Rekenkamer'). In it's report 'E-health, an innovation in long-term care' ('Zorg op afstand. Een innovatie in de langdurige zorg'), the Court of Audit concludes that the care sectors have too few incentives to encourage innovation and the dissemination of innovations. Furthermore, legislation, and regulations also hold back the dissemination of care innovations, for example,

[17] Seehttp://www.nveh.nl/index.php?option=com_content&view=article&id=86&Itemid=100. Accessed 21 December 2009.

[18] Seehttp://www.tno.nl/downloads/Manifest_eHealth_v4a.pdf. Accessed 21 December 2009.

because of the medical/legal issues at stake and the uncertainties at play.[19] In this respect, the Court of Audit recommends to identify medical and legal issues, and uncertainties so that changes in the law and regulations can be considered.

In December 2009, the Royal Dutch Medical Association (KNMG) started a virtual eHealth Community to be used by and for doctors only. The purpose is to create a platform for exchanging eHealth experiences between doctors, for asking questions and finding answers about eHealth, finding relevant information and for discussions.

The strategy behind these initiatives is to stimulate health innovations. eHealth services could contribute to enable society to deal with the social problems that are caused by the growing number of chronic patients and elderly with health problems. These social problems will occur because of the growing scarcity of employment and the rising costs of healthcare, at the same time. It is firmly believed that the right innovations could support traditional health care and play an important part in solving these social problems.[20]

16.2.3.1 Examples of Dutch eHealth Applications

In this section, we will describe just a, few examples, of eHealth applications in the Netherlands. A number of other examples could also have been mentioned, like patient portals to access one's own patient data (Lindenholt Nijmegen, Mijngezondheid.net, Medischegegevens.nl, Mijnflevoziekenhuis.nl), websites that provide medical information for patients (e.g., www.fhbosch.nl, www.mijnspecialist.nl), and interactive consultation services by e-mail (www.emaildokter.nl) and Twitter (@tweetspreekuur: twitter.com/tweetspreekuur).

16.2.3.2 TCCN ('Stichting Teledermatologisch Consultatie Centrum')[21]

The Teledermatological Consultation Centre Netherlands (TCCN) is a foundation that offers a teleconsult for a dermatological problem. The General Practitioner (GP) of a dermatology patient makes a digital picture of the skin problem. The GP logs on to the website www.teleconsultatie.nl with his username and password. Together with a questionnaire (anamnesis), the GP sends the pictures by e-mail to a dermatologist. The dermatologist receives the e-mail message and possibly an SMS text message that he received a request, and he logs on to the TCCN website.

---

[19] See http://www.courtofaudit.com/english/News/Audits/Introductions/2009/06/E_health_an_innovation_in_long_term_care. Accessed 21 December 2009. On 11 June 2009, this report was submitted to the House of Representatives.

[20] Seehttp://www.tno.nl/downloads/Manifest_eHealth_v4a.pdf (Manifest TNO). Accessed 21 December 2009.

[21] Seehttp://www.teleconsultatie.nl/. Accessed 21 December 2009.

The dermatologist makes a diagnosis, and he returns the results to the GP together with a therapeutic advise. The GP receives the e-mail message and possibly an SMS text message that his questions have been answered, and he logs on to the TCCN website.

16.2.3.3 Virtual Thrombosis Service[22]

The Virtual Thrombosis Service Foundation is an official thrombosis service that offers health services to patients by means of internet, e-mail, mobile, and fixed telephony. Patients are trained on the internet how to measure their coagulation values by means of a measure device, to calculate their dosage schedule themselves, and to build their personal electronic health record. Through the website, the patient can store these values, contact the thrombosis doctor, and have easy access to his record from anywhere in the world. The Virtual Thrombosis Service operates at a national level (not just regional). Patients from all over the country can apply to this service.

16.2.3.4 ZorgDomein[23]

The internet-referral-application 'ZorgDomein' improves the synergy of demand and supply between primary and secondary healthcare. ZorgDomein tries to build a bridge between the General Practitioners (GP) and the hospitals, the mental healthcare and other secondary healthcare professionals. The purpose is to inform the patient and his GP better, to improve the communication between professionals in the healthcare chain, to have the patient at his appointment faster, and to prevent unnecessary visits of the doctor. The working method behind ZorgDomein, introduced in over 30 hospitals in the Netherlands, resulted in significant improvement in the efficiency of care as well as in the service to patients.

16.2.3.5 Portal Website for Invitro Fertilization Treatment

In 2002, the Department of Obstetrics and Gynecology and the Department of Medical Informatics of the Radboud University Medical Center, established the portal website for IVF treatment.[24]

---

[22] Seehttp://www.virtueletrombosedienst.nl/vtdfront. Accessed 21 December 2009.

[23] See https://www.zorgdomein.nl/zorgdomein/opencms/www/home/english.html (see also Good eHealth Practice in EU> NL, p. 37). Accessed 21 December 2009.

[24] Sources: European Commission 2009. European Commission, Information Society and Media, Good eHealth. Exchange of Good Practices on eHealth—Knowledge Base http://www.good-ehealth.org

Patients visiting the website have access to all necessary medical information and are given support to interpret this information. The website also enables online communication between patients and their physicians.

The website's content contains general information about infertility and the IVF treatment. Secondly, it provides patients with personalized information, mainly by giving the patients, access to their own medical records. Thirdly, the website offers a number of communication options, including e-mail facilities, a discussion forum (bulletin board), and a chat room. Physicians actively participate in the latter two, to moderate the discussions, to answer the patients' questions, and correct faulty information.

In May 2005, the Portal website for IVF treatment was 'Case of the Month' on the EU website Good eHealth.[25]

16.2.3.6 I.COM: Mental eHealth[26]

I.COM is the Innovation Centre of Mental Health and Technology and is part of the Trimbos Institute. I.COM aims to promote the use of mental eHealth to improve the quality and accessibility of care for people with psychological problems. Recently, I.COM started the program 'Mentaal Vitaal' (Mentally Vital). This innovative program includes 13 projects and 6 new web-based interventions. The purpose of 'Mentaal Vitaal' is to ensure that the least possible number of people suffer from a depression. Therefore, 'Mentaal Vitaal' uses new technologies and methods that are applied through the internet.

I.COM states that mental eHealth can reach as many people as possible. Benefits of e-health for mental disorders are that interventions can be designed in accordance with the best available evidence, be well structured, and involve people interactively; e-therapy may be helpful for patients who otherwise would be hard to reach for the traditional mental health services; therapists' involvement can often be kept to a minimum, thus freeing up much of limited resources such as therapists' time; the interventions can be delivered on a broad scale via the internet, independent of time and place like in the privacy of their house, or also via stand-alone computers in clinics, hospitals, and primary care posts.[27]

16.2.3.7 National Electronic Health Record

The Dutch Ministry of Health, Welfare and Sports is working on the introduction of a national Electronic Health Record (EHR) system (EPD).[28] This EHR system

---

[25] See, e.g., UMC St. Radboud, Digitale IVF-poli 'Case of the month' http://kb.good-ehealth.org/browseContent_alt.do?contentId=49&action=v3. Accessed 21 December 2009.

[26] See http://www.icom.trimbos.nl. Accessed 21 December 2009.

[27] I.COM Innovation Centre of Mental Health and Technology.

[28] Ministry of Health, Welfare and Sport 2006.

will consist of a secure network environment in which patient data, stored in different local health systems (e.g., at the GP), can be retrieved by other authorized healthcare providers for healthcare related purposes. This virtual health record (EPD) consists of a collection of applications, which are connected to a national information infrastructure called AORTA. It will not consist of a central database.

To provide healthcare providers with a facility for calling up patient data, a National Switch Point (LSP) has been built, providing a reference index for routing, identification, authentication, authorization, and logging. This LSP acts as a 'traffic control tower' for the calling up of patient data from the health information systems of hospitals, pharmacies, and GP's. To guarantee that the patient data are well secured and systematically stored, these local information systems have to meet the criteria for a Well-Managed Healthcare Information System (GBZ).

The Dutch government has opted for an incremental development of the EHR. The first two 'chapters' of the EHR will consist of an Electronic Medication Record (EMD) and the Electronic General Practitioner's Record (WDH). Other 'chapters' or records are being developed, like an Electronic Emergency Record and a Electronic Diabetes Record.

The healthcare providers have the primary responsibility for the quality of healthcare and the use and quality of the patients' data in their health information systems. The government is responsible for paving the way by passing legislation, creating the right investment climate, and coordinating the overall process.

16.3 The European Legal Framework for eHealth

16.3.1 Introduction

Despite all efforts in policy making both at EU- and national level, the providers of the eHealth services mentioned in the second part of Sect. 16.2, must still be considered front runners. The provision of eHealth services is still not as widespread, as one would expect considering it's possibilities. In Sect. 16.2 we mentioned, that legal certainty for suppliers and users is important to the further development of eHealth. Legal certainty about their positions will stimulate suppliers to research and invest in new developments and will also have a positive influence on consumer confidence. In this section, we will investigate these legal issues surrounding the use of eHealth tools.[29]

The scope of legal issues relevant to eHealth is a wide one, ranging in general from, for example, contract law, employment law to even criminal law. In its Communication on telemedicine,[30] the European Commission mentions issues like accreditation, liability, reimbursement, privacy, and data protection as

[29] See also European Commission 2008a.

[30] Commission of the European Communities 2008c.

examples of issues that should be addressed in the legislation of the Member States. In this section, we will focus on (1) privacy and data protection, (2) product and services liability, (3) competition law, and (4) patient rights, patient safety, and quality of care. To a certain extent, these issues differ from the legal issues mentioned in the EC Communication. They are however the central issues that can be found in documents[31] and literature on eHealth (Callens 2009). The issues differ only slightly from the ones mentioned in the Communication: the issue of reimbursement will be addressed in the context of competition law. Accreditation is an issue that we will address in the context of privacy and data protection, as well as patient safety.

16.3.2 The European Legal Framework

Traditionally the legal framework in the healthcare domain was completely set by the national legislators. In traditional medicine, where a physician takes care of the patient in his local practice or hospital and the national health insurance pays for the treatment, there seems to be little need for supranational regulation. In today's world of healthcare, patients as well as healthcare workers, more and more cross their national borders (Callens 2009). Patients use the internet to consult a doctor and doctors increasingly use ICT tools to consult with other healthcare professionals in the course of treating their patients. By their nature, eHealth and telemedicine can make it easier for both patients and healthcare workers to cross their national borders and search for the best healthcare, regardless of the place where to find it.

Considering this, eHealth seems to be an area par excellence, for the European legislator to set out the legal framework. However, when looking at the European legal framework, it is important to realize that healthcare as such is not the sole domain of the European Union (EU). Where the EU has exclusive competence in matters of, for example, the customs union and common commercial policy,[32] the EU has to share competence with the Member States in public health matters[33]: in matters of the protection and improvement of health of the European citizens, the EU has the competence to support, coordinate, and supplement the actions of the Member States.[34] Although with the ratification of the Treaty of Lisbon, the promotion of the well-being of its people has become an important aim of the Union,[35] the primacy in health and healthcare matters lies with the national legislators.

---

[31] European Commission 2008a.

[32] Art. 3 consolidated version of the Treaty of the functioning of the European Union. OJ C115 of 9 May 2008 (hereafter TFEU).

[33] Art. 4, paragraph 2, sub k, TFEU.

[34] Art. 6, sub a, TFEU.

[35] Art. 3, consolidated version of the Treaty on the European Union. OJ C115 of 9 May 2008 (hereafter TEU).

Table 16.2

Data protection and privacy	Data Protection Directive (95/46/EC)
Product and services liability	General Product Liability Directives (2001/95/EC and 1999/34/EC)
	Directive on Distance Contracting (97/7/EC)
	General Product Safety Directive (2001/95/EC)
	Medical Device Directives (93/42/EC, 90/385/EC, 98/79/EC, and 2007/47/EC)
	Defective Products Directive (85/374/EC)
	eCommerce Directive (2000/31/EC)
European Competition Law	Articles 81–89 Treaty establishing EU
Patients' rights: access to healthcare and quality of care	Proposed Directive on patients' rights in cross-border healthcare (COM(2008), 414 final)
	Directive on the recognition of professional qualifications (2005/37/EC)

Yet in Sect. 16.3.1 we saw that the legal issues surrounding eHealth are not just of healthcare nature. We identified the main legal issues surrounding eHealth, being:

- Patient data protection, privacy and professional confidentiality
- Product and services liability
- Trade and competition law
- Patients' rights, patient safety, and quality of care

Some of these surrounding issues are in the domain of the EU legislator and by regulating these issues, the EU-legislator can and does influence the legal domain of eHealth. In the next sections we will give an overview on the European legal framework with regard to these legal issues.

For the topics we will cover in short, see Table 16.2.

16.3.2.1 Patient Data Protection, Privacy and Confidentiality

Most eHealth applications will involve the collection and processing of information regarding an identifiable patient.[36] Such information is legally known as personal data and is subject to data protection legislation in the EU. The main European source of data protection is Directive 95/46/EC (hereafter Data Protection Directive).[37] The Data Protection Directive has two main purposes:

[36] See also European Commission 2008a, pp. 14 et seq.

[37] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995.

firstly to protect the fundamental rights and freedoms of the person to whom the data relate. These persons are called 'data subjects.' Secondly the Directive aims to allow the free movement of personal data within the EU in the context of the internal market.

The Data Protection Directive consists of a set of rules that a person or legal entity collecting or processing personal data has to meet. These obligations mainly concern the so called data controller: the person or organization who determines the purpose and means of the data collection. The set of rules contains eight basic data principles. The data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

To the processing of special categories of data, also called 'sensitive data,' extra restrictions of data protection apply. Data concerning a person's health are considered as sensitive data. In short, the processing of these data is only allowed for reasons related to the medical treatment by national competent bodies and by persons subject to an obligation of professional secrecy.

Next to the rules applying for data controllers, the Directive also gives certain rights to the data subjects. From the eHealth perspective these data subjects are of course usually patients. The patients have the right:

- To request specific information about their own personal data
- To have the data rectified when they are incorrect or incomplete
- To object to the processing of their data under certain conditions

All EU Member States have implemented the Data Protection Directive in their national legislation.

16.3.2.2 Product and Services Liability

When using eHealth applications, ranging from Electronic Health Record systems to telemonitoring devices (domotics, or home automation) enabling the elderly to live on their own longer, both professional users as well as patients (or consumers) expect to be protected by law, if an eHealth product or service does not work properly and subsequently maybe even cause damage to a patient. Does the European legal framework supply this protection?

Regarding this question, it is important to realize that currently there is no specific European legislation targeting eHealth services.

16.3.2.3 General Contract Law and Consumer Protection

Just like the buying and selling of traditional products, the buying and selling of eHealth products is covered by general contract law.[38] The General Product Liability Directives (Directive 2001/95/EC[39] and Directive 1999/34/EC)[40] form the basis for national law in the Member States, ensuring that the purchaser of a consumer good has redress, if the goods are delivered late. Also Directive 1999/44/EC[41] on the sale of Consumer Goods enables the consumer purchaser of an eHealth device to pay less or return the good, when it isn't fit for its purpose. These Directives not only ensure that the seller or producer of consumer goods must deliver goods as described in the contract of sale, but also ensure that existing commercial guarantees as well as the associated advertising are legally binding.

If the use of an eHealth Product involves the conclusion of a contract at a distance, it may also be subject to the Directive on Distance Contracting (Directive 97/7/EC).[42] Among other obligations this Directive imposes on the supplier, the obligation to provide the recipient with written information about his identity, product, and price, prior to the conclusion of the contract.

In some cases, it might be unclear whether consumer protection rules are applicable. For example, when the patient is not the buyer of the eHealth product, but only uses it.

16.3.2.4 Product Safety

The General Product Safety Directive (2001/95/EC) imposes a general safety requirement for any consumer product put on the market. Producers must give consumers information enabling them to assess the risks adherent to the product and are, for example, also obliged to take appropriate measures to avoid these risks.

---

[38] European Commission 2008a.

[39] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety. OJ L 11, 15.1.2002, pp. 4–17.

[40] Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products. OJ L 141, 4.6.1999, pp. 20–21.

[41] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees. OJ L 171, 7.7.1999, pp. 12–16.

[42] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts—Statement by the Council and the Parliament re Article 6(1)—Statement by the Commission re Article 3(1), first indent. OJ L 144, 4.6.1997, pp. 19–27.

16.3.2.5 Liability for Damages by an eHealth Device

Products

Directive 85/374/EC on Defective Products[43] aims to ensure a high level of consumer protection against damage to health or property caused by a defective product. The Directive establishes a 'no-fault liability' for damage caused by a defective product. Thus the injured person does not have to prove that the producer was negligent, he simply has to prove that the damage was caused by the defect of the eHealth product for the producer to pay his damages.

To strike a balance between producers' legal certainty and consumer protection, this liability is limited to three year period from the moment a consumer is aware of the damage, the defect, and the identity of the producer. The no-fault liability expires overall ten years after the product is being put on the market.

Services

In many situations the delivering of eHealth services will imply that the physician providing advice to patients will rely on an eHealth support tool. The failure of this support tool, being, for example, a failure in external support-software or a defect of the monitoring device, can cause a doctor to give a wrong advice. Clearly this might cause serious damage to a patient's health. The patient's claim on the doctor in such a case will be based on services liability. In his turn, the doctor relying on this defective product might have a claim based on the Defective Products Directive mentioned above.

To the patient's claim or if a default decision or doctor's advice has no direct link to a defective product, of course this Directive does not apply. Legally we speak of services or professional liability in a situation like that. Currently there is no general European harmonization of liability rules for services; whether liability exists, is determined by the ordinary rules of law applicable in the Member States.[44]

An exemption to this may be eHealth applications that meet the qualifications of an information society service. Those remunerated services at a distance at the specific request of a recipient provided wholly by electronic means are covered by the e-Commerce Directive (2000/31/EC).[45] In the eHealth domain, this Directive

---

[43] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products. OJ L 210, 7.8.1985, pp. 29–33.

[44] The proposed Directive on the application of patients' rights in cross-border healthcare COM (2008) 414 final, does have a provision on the applicable law. See Sect. 16.3.2.4.

[45] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). OJ L 178, 17.7.2000, pp. 1–16.

applies to, for example, the online selling of medication or online medical advice that is paid for and does not require the physical examination of a patient, but also to websites of doctors promoting their activities. The Directive imposes certain information obligations to the service provider to allow users to seek redress if necessary.

In general, the rules of the country in which the service provider is registered will apply. The provider therefore is obliged to put this information on the website. Exemptions to this 'country of origin principle' may be made by Member States, for example, if this is necessary to protect public health.

16.3.2.6 European Competition Law

Until fairly recently, the provision of healthcare services was not considered a service within the scope of competition law. Historically, healthcare was generally conceived as an intellectual service provided by professionals requiring certain skills not suitable for separation into different economic activities subject to competition.[46] However, in the last few decades, the provision of healthcare services has become a factor of economic interest arousing the interest of competition lawyers. In 1998, the European Court of Justice established new principles through its rulings in two cases[47] regarding direct application of Treaty articles on free movement to the reimbursement of health services provided to patients abroad. According to this case law national health insurers are not allowed to refuse an insured person the reimbursement of medical products or services acquired in another Member State, if they would reimburse those same products or services when acquired nationally.

Does this case law have implications for the trade in eHealth tools and the way they are made available to the public?

In the provision of healthcare, the support of technical services by specialized providers that are not necessarily medical professionals becomes more and more important. These providers will seek to provide their special services in an international open market. Therefore, competition law in healthcare and especially in eHealth is likely to become more and more important in the near future.

When a provider offers an eHealth service directly to consumers in an open market, there will be little doubt that these activities are subject to competition law.

However, often eHealth services provided by commercial parties are not directly sold to consumers. In some situations the services or applications are sold to public hospitals or healthcare insurers, who in their turn will make these services available to the patient. In most Member States, those hospitals or healthcare insurers are, at least partly, funded by the government. It is still not completely

[46] European Commission 2008a.

[47] Case C-158/96 Kohl (1998) ECR I-1931 and Case C-120/95 Decker (1998) ECR I-1831.

clear if and if so, to what extent the rules of competition law apply to those (partly) publicly funded bodies.

16.3.2.7 What does European Competition Law Imply?

European competition law aims to create a level playing field for the economic activities of commercial businesses across the European Union. This creation of an internal market, where commercial activities can be deployed freely regardless of the European country of origin and without too much restrictions of national or regional authorities or anticompetitive actions on the part of other companies, is of course one of the European Union's core businesses.

The basis of European competition law is Article 3(b) of the Treaty on the Functioning of the European Union. This provision aims to create a system ensuring that competition in the internal market is not distorted. European competition law applies to issues affecting the intra-community trade; in most cases national competition law will also apply next to European law.

The system ensuring that competition in the internal market is not distorted is elaborated further in the Articles 101–109 of the Treaty of the functioning of the EU (TFEU).[48] The core of European competition law is in the first two articles of this section: Article 101 prohibits agreements between private companies or enterprises and concerted practices with an anticompetitive object or effect on the internal market. Article 102 prohibits the abuse of a dominant position in the market. A little further on, Article 106(2) states that these rules also apply to public enterprises (known judicially as 'undertakings') as long as the applicability of the rules does not obstruct the performance of the tasks assigned to them.

The question is whether partly publicly financed hospitals, health insurers or other healthcare providers can be classified as such an 'undertaking.' The key factor in assessing this, is whether the organization is engaged in any economic activity. Case law of the European Court of Justice[49] rules that a purchasing activity is not subject to competition law if it is undertaken for purely social purposes. In the *FENIN* case the court ruled that a publicly funded chain of Spanish hospitals was not engaging in economic activities while purchasing large amounts of goods from the market for use in the hospitals providing free-of charge service on the basis of universal insurance coverage. A healthcare provider, however, operating outside these criteria—for example when offering extra services for remuneration outside the basic insurance package—could well be classified as an 'undertaking' and thus be subject to competition law, which means that the healthcare provider has to comply with the Articles 101 and 102 of the Treaty, of the functioning of the EU.

---

[48] Before the Treaty of Lisbon, the Arts. 81–89 Treaty of the EU (old) contained the competition rules.

[49] *FENIN* v. *Commission of the European Communities*, 11 July 2006, Case C-205/03.

However, even when a healthcare provider is qualified as an 'undertaking' engaging in economic activity, it can be exempted from having to comply with the aforementioned obligations. It might be possible for the healthcare provider to operate outside the Articles 101 and 102, if the provider has been entrusted by a public body to deliver Services of General Economic Interest (SGEI). Article 106 TFEU allows 'undertakings' providing SGEI's to be exempted from the rules of competition law, if the application of those rules would obstruct the performance of the particular tasks assigned to them. The Treaty does not define SGEI's. Instead, Member States define what they consider to be an SGEI and only if there is a manifest error, the European Commission and the Court of Justice will review these definitions. An SGEI is usually a service:

- That the market does not provide, at least not to the extent the State deems necessary
- That is capable of being carried out on a commercial basis
- That is in the general interest and is delivered to the public at large

Under certain conditions eHealth tools provided to the public at large could be qualified as an SGEI.

16.3.2.8 Patient's Rights, Patient Safety and Quality of Care

In the Sects. 16.3.2.2 and 16.3.2.3 we saw that the development of eHealth and providing of eHealth tools can have aspects of commercial trade on a free market and providing goods and services to consumers on demand. Yet the provision of eHealth tools to the public, first and foremost is also part of healthcare.

Being part of healthcare, the use and provision of eHealth tools also raises questions in the domain of health law. What are the consequences of the applicability of patients rights to the providing and use of eHealth tools? Do obligations and legal standards on patient safety and quality of care have implications for the use of eHealth tools? And do health insurers provide or reimburse the use of eHealth?

Cross-Border Healthcare

The EC is aware that high-quality health services are a priority for European citizens.[50] Rights to healthcare are also recognized in the Charter of Fundamental rights of the EU.[51] Yet as described in the first part of this section, the primary

[50] Communication from the commission, Consultation regarding Community action on health services, Brussels, 26 September 2006, SEC (2006) 1195/4.

[51] Art. 35 Charter of Fundamental Rights of the European Union. OJ C 364, 18.12.2000, pp. 1–22.

responsibilities in regulating the healthcare domain lies with the Member States. The EC competence in this domain is restricted to the support, coordination, supplementation of the national Member States' actions.

Nevertheless, the European Court of Justice ruled that Treaty provisions on free movement apply to the reimbursement of health services.[52] These rulings raised questions among stakeholders about the application of community law to health services and healthcare.[53] In an attempt to provide legal clarity and to codify the Court's rulings the EC has drafted a proposal for a 'Directive of the European Parliament and of the Council on the application of patient's rights in cross-border healthcare.'[54] On January 19th 2011, the European Parliament adopted an amended version of the Directive in second reading. (A provisional edition of the text adopted by the European Parliament is published on www.europarl.europa.eu under document number P7_TC2-COD(2008)0142.) The proposal will be considered by the EU Council of Ministers in March 2011, before it can be officially adopted.

Based on the aforementioned case law and Article 95 of the Treaty, the initiative aims at ensuring a clear and transparent framework for the provision of cross-border healthcare within the EU, for those occasions when the care to patients is provided in another Member State than their home country. In those cases there should be no unjustified obstacles to access healthcare and the procedures for reimbursement should be clear and transparent. Also the necessary requirements for high-quality, safe, and efficient healthcare should be ensured for situations of cross-border healthcare.

The proposed Directive states that the 'Member States of treatment' are responsible for the organization and the delivery of healthcare, but also requires them to define clear quality and safety standards for healthcare, including, for example, the right of patients to complain and compensation upon harm arising from healthcare and a system of professional liability. One of the essential provisions in the Directive is that Member States shall not make the reimbursement of costs of regular planned healthcare provided in another Member State subject to prior authorization. Only when the care requires overnight accommodation, or the use of highly specialized or cost-intensive medical infrastructure or equipment, or presents a particular risk for the patient or the population, a prior authorization may be required.[55]

The proposed Directive also defines the applicable rules to healthcare provided in another Member State, than, where the patient is insured: the legislation of the Member State of treatment applies.[56] The Directive as adopted by the European Parliament in second reading holds a specific provision for care delivered by

---

[52] See the rulings mentioned in note 47.

[53] European Commission, COM (2006) 122.

[54] COM (2008) 414 final. Proposal for a Directive of the European Parliament and of the Council on the Application of Patients' Rights in Cross-Border Healthcare, 2008/0142 (COD).

[55] However in the most recent proposal, the Directive does not apply to long-term care whose purpose it is to support people in need of assistance, of every day routine tasks.

[56] Art. 4 Proposed Directive on the application of patients' rights in cross border healthcare.

means of telemedicine. Article 3d of this version of the Directive states: "In the case of telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established."

The proposed Directive on cross-border healthcare explicitly addresses eHealth. The Directive requires the Union to support and facilitate cooperation and the exchange of information among Member States, working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States. In this voluntary network, the Member States should work towards a high level of patient trust and safety in healthcare. This—regretfully only voluntary—network should identify a list of data to be included in patients' summaries that can be exchanged between health care providers across borders and support Member States in facilitating the transferability of data in cross border health care. The proposal does not oblige any introduction of eHealth systems or services, as is stated in the explanatory memorandum, but aims at ensuring interoperability of Member States' information and communication technologies, once a Member State decides to introduce an eHealth service.

Medical Devices

When an eHealth device is designated as a medical device by its producer, also the Medical Device Directives apply. The General Medical Device Directive (Directive 93/42/EC)[57] aims to protect the health and safety of patients, and users by harmonizing the conditions for introducing medical devices in the market. Directive 90/385/EC[58] applies for active implantable medical devices. The third Directive on this issue, Directive 98/79/EC[59] deals with in vitro diagnostic devices. When an eHealth device is used to dispense a medicinal product, Directive 2001/83/EC[60] applies and requires a prior marketing authorization for compound dispensed by the device. In September 2007, Directive 2007/47/EC was published.[61] This directive amends both Directives 93/42/EC and 90/385/EC and has to be applied by 21 March 2010.

---

[57] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices. OJ L 169, 12.7.1993, pp. 1–3.

[58] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices. OJ L 189, 20.7.1990, pp. 17–36.

[59] Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices. OJ L 331, 7.12.1998, pp. 1–37.

[60] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use. OJ L 311, 28.11.2001, pp. 67–128.

[61] Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market. OJ L 247, 21.9.2007, pp. 21–55.

Continuing research and development almost inevitably will result in more and more eHealth products being qualified as medical devices. Considering the growing possibilities in, for example, implantable monitoring devices, it is likely that the importance of this legislation will also grow.

Professional Qualifications

Another element of the European legal framework bordering 'quality of care' issues, is Directive 2005/36/EC, the directive on the recognition of professional qualifications.[62] This Directive establishes rules according to which a Member State that makes access to or pursuit of a regulated profession, including health professions, in its territory contingent upon possession of specific professional qualifications, shall recognize professional qualifications obtained in another Member State enabling the qualifier to pursue the same profession there.

16.4 A Dutch Analysis of the European Legal Issues

16.4.1 Introduction

The Dutch healthcare system has a private character with social conditions (Eijpe 2008). The system is operated by private health insurance companies. According to the Health Insurance Act ('Zorgverzekeringswet' or Zvw), every resident in the Netherlands has a legal obligation to take out insurance. The insurance companies have the obligation to accept every resident for the standard insurance package, irrespective of age or state of health. The health insurance consists of a standard package of essential healthcare.

Apart from the free choice of insurers, the citizen has the following other choices:

- The level of the nominal premium
- The type of policy (care in kind or refund of costs) and the service provided by the insurer
- The level of the voluntary excess: from € 0 to € 500
- The option to take out supplementary insurance for care that is not included in the standard package (e.g., dental treatment or alternative medicine)

[62] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (Text with EEA relevance). OJ L 255, 30.9.2005, pp. 22–142.

Next to the standard insurance package and the optional supplementary insurance, a third compartment of insurance covers the long-term care.[63] This compartment provides the insured with chronic and continuous healthcare, which involves considerable financial consequences, such as care for disabled people with congenital physical or mental disorders.

Access to healthcare is guaranteed by the independent Healthcare Insurance Board ('College voor Zorgverzekeringen' or CVZ). The CVZ coordinates the implementation and funding of the Health Insurance Act (Zvw) and the Exceptional Medical Expenses Act (AWBZ). Among other tasks, the CVZ advises the government about the content of the standard insurance package. They see to it that the standard insurance package contains all the necessary healthcare, and that everybody is informed about it.

For this analysis, we think it is relevant to point at a number of future legislative developments. In February 2009, the Dutch House of Representatives accepted the national Electronic Patient Record Bill ('Kaderwet EPD').[64] This Bill proposes a change in the Act on the Use of the Citizen Service Number in Healthcare ('Wbsn-z'). In February 2011, the Bill was still pending in the Senate. The Bill addresses issues like security, data quality, authorization and access, standardization, and the actual use of the nationwide Electronic Patient Record. The Bill regulates the mandatory connection of (categories of) healthcare providers to the National Switch Point (LSP), the electronic availability of patient data via the LSP, and the security and reliability of the exchange of patient data via the LSP. It is possible that, after the acceptance of the Bill by the Senate, a number of provisions will not come into force immediately.

Another possible important future legislative development is the introduction of the 'Client Rights' in Healthcare Bill ('Wet cliëntenrechten zorg'). This Bill was introduced by the government into parliament on 7 June 2010. The Bill proposes to collect all the rights of patients and clients, and the obligations for healthcare providers and professionals in the cure and in the care together in one Act.

16.4.2 Patient Data Protection, Privacy, and Confidentiality

The EU Data Protection Directive 95/46/EC, has been implemented in the Personal Data Protection Act ('Wet bescherming persoonsgegevens' or WBP), which came into force on 1 September 2001. The WBP is very similar to Directive 95/46/EC. The WBP contains the following general principles:

---

[63] Exceptional Medical Expense Act (AWBZ). See: http://www.minvws.nl/en/themes/exceptional-medical-expenses-act/default.asp. Last modified: 13 March 2007.

[64] Amendment of the Act on the Use of the Citizen Service Number in Healthcare in the context of the Electronic Exchange of Information in Healthcare ('Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg'). Kamerstukken 31466.

- Processing of personal data must be in accordance with the law, fair, and lawful (Art. 6)
- Collection of personal data is only allowed for specified, explicit, and legitimate purposes (Art. 7)
- Processing of personal data must be legitimate (Art. 8)
- Further processing of personal data should not be incompatible with the purposes for which they were collected (Art. 9)
- Personal data must be adequate, relevant, and not excessive in relation to the purpose for which they were collected (Art. 11)
- Personal data must be secured by adequate measures (Arts. 12, 13, 14)
- Personal data are no longer kept in a form which permits identification, than is necessary for the purposes for which they were collected (Art. 10).

The processing of sensitive data is subject to special legal conditions (Hooghiemstra and Nouwt 2007, pp. 21–22).

The WBP also provides general (privacy) rights for data subjects. These include the patients' rights to personal data. However, also specific legislation exists with patients' rights to medical records. Because the Dutch healthcare system is a private system, these patient rights are recognized in a separate chapter of the Dutch Civil Code ('Wet geneeskundige behandelingsovereenkomst' or WGBO). Because the WGBO is a Special Act in relation to the WBP, these patient rights in the WGBO precede over the data subject rights in the WBP. Article 7:457 WGBO provides that healthcare providers are not allowed to disclose personal information about the patient to a third party. As a result, this obligation of medical confidentiality precedes over the legitimate processing of patient data.

For telemedicine applications, including teleradiology, teleconsultation, etc., the data protection rules must be applied when personal data are being processed. This means, in the first place, that there should be a legal justification to exchange patient data while respecting the rule of medical confidentiality. In the second place, the exchange of patient data must be in accordance with the general and specific principles for the processing of medical data. Thirdly, the controller has an obligation to comply with the administrative procedures of the WBP, like the obligation to inform the patient, to notify the national supervisory authority, and to take adequate security measures.

When doctors are using the national Electronic Health Record system, they will have to comply with the (future) legal obligations in the Electronic Patient Record Act ('Kaderwet EPD'), which elaborates the rules of medical confidentiality and data protection. Examples of these obligations are:

- To connect their health information system to the LSP
- To record and maintain patients' index data
- To record and maintain patients' health data in their information system
- Disclose a patient's data via the LSP at another doctor's request
- The doctor's health information system must meet the GBZ standards

Recently, from this legislative perspective, the national health record system had quite a lot of legal and social attention. According to one of the members of the House of Representatives, they seem to have been sleeping with regard to the legal framework while in the meantime local and regional health information records were developed.[65] This could illustrate the legislator's focus on large scale developments, while forgetting the small scale. It would be better to prevent this from happening with regard to other eHealth applications, in order to provide legal certainty for all eHealth applications.

16.4.3 Product, Services, and Professional Liabilities

In the Netherlands, a doctor can be held liable on several legal grounds. His liability can be based on civil law, criminal law, disciplinary law, privacy law, and complaint law. Based on civil law, a doctor can be held liable for causing damage to the health or the privacy of a patient. A doctor runs a small risk of criminal liability for faults in the medical treatment or for breaking his obligation of medical secrecy. The disciplinary liability for health professionals (doctors, nurses, etc.) is regulated in the Individual Healthcare Act ('Wet BIG'). For privacy law, a doctor can be liable for non compliance with the Personal Data Protection Act (WBP). For small complaints, doctors can be subject to a complaint procedure based on the Client's Right of Complaint (Care Sector) Act (WKCZ).

According to Dutch civil law, a health professional is not only liable for his own acting, but also for damage caused by his subordinates (Art. 6:170 Civil Code), non-subordinates and providers (Art. 6:171 Civil Code), representatives (Art. 6:172 Civil Code), and by assisting persons and products (Arts. 6:76 and 6:77 Civil Code). In Dutch law, the producer of an eHealth device is also liable when damage is caused to a patient by a defective product.[66]

A number of EU directives created a legal framework for electronic commerce in Europe: Directive on Distance Contracts (97/7/EC), Directive on Electronic Signatures (99/93/EC), Directive on Electronic Commerce (2000/31/EC), and the Directive on Distance Marketing of Consumer Financial Services (2002/65/EC). For example, the directives on distance contracts and electronic commerce have been implemented in the Dutch Civil Code by the Distance Contracts Act (Book 7 Civil Code), and by Electronic Commerce Adaptation Act, which especially regulates the information society 'services,' including the selling of goods online (Book 3 and 6 Civil Code). An electronic (online) contract can be considered a specific kind of a distance contract.

Apart from a number of general provisions on distance contracts, the Distance Contracts Act implemented the right to revocation and the information obligations

[65] Handelingen II, 56, p. 4488 (18 February 2009).

[66] Art. 6:185 Civil Code.

of the provider in the Civil Code. These provisions are applicable to the delivery of goods and services (see e.g., Sander 2001).

The Electronic Commerce Adaptation Act regulates, among other things, that a service provider who is established in the Netherlands, is legally committed against recipients of his service to Articles 3:15d (general information obligation), 3:15e (commercial communications), 6:227b and 6:227c (electronic contracting) (See e.g., Esch van 2004).

16.4.4 Competition Law

The Dutch Healthcare Authority (NZa) is the supervisory body for the Dutch healthcare markets. The NZa supervises both healthcare providers and insurers, in the curative markets as well as the long-term care markets.[67] The NZa derives its tasks from the Healthcare Market Regulation Act ('Wet marktordening gezondheidszorg' or Wmg).

The NZa could play an important role in this era of aging population, growing need for healthcare, and technological innovations. As the healthcare market supervisor, the NZa gets the new markets going that emerge in the healthcare sector whenever it can. These could include eHealth markets. The NZa plays this role to provide consumers with accessible, affordable, and proper healthcare.

Competition law is important for the regulation of the healthcare market. Competition law is primarily developed for companies. But also Member States are not allowed to act against provisions of competition law. However, Member States can back out public interests of the economic market rules by appealing to the concept of Social Services of General Interest (SGEI) (see e.g., Gronden van de, and Sluijs 2009). It is the national government that decides that a certain service is to be considered as an SGEI, including its content. Services of general interest can cover a broad range of activities: energy, telecommunications, postal services, transport, and also health.[68] They are services that are essential in daily life of citizens and enterprises. The Dutch healthcare insurance companies qualify as an SGEI enterprise (see e.g., Gronden van de, and Sluijs 2009). However, it is not clear whether healthcare providers can be considered as SGEI enterprises. There is no European case law or Commission decision. According to the Netherlands Competition Authority (NMa), healthcare providers are normal enterprises. An interesting question is, whether providers of eHealth can become enterprises who deliver SGEI's in the near future.

[67] Source: http://www.nza.nl/nza/#

[68] Commission of the European Communities 2007a.

16.4.5 Patient Safety and Quality of Care

In 2005, research showed that in the Netherlands several healthcare providers, knowledge institutes, suppliers and manufacturers were active in implementing domotics applications (Jong de and Kunst 2005). The researchers concluded that there is a lack of a healthcare, legal, and social framework for domotics to comply with. It is important to provide these frameworks and (legal) clarity on responsibilities and liabilities in order to ensure the quality of health care delivered and to prevent life threatening situations.

Producers of medical devices have an obligation to ensure patient safety, which is guaranteed by the Medical Devices Act ('Wet op de medische hulpmiddelen').[69] This Act is the implementation of the General Medical Device Directive (93/42/EC). The Medical Devices Act introduces a permit system, prescriptions and requirements, and also the criminal liability for recommending defective medical devices. The Medical Devices Act is a framework act and is the basis for several administrative orders, like for example:

- Medical Devices Decree
- Active Implantable Medical Devices Decree
- In Vitro Diagnostics Decree

Since 1993, the Individual Healthcare Act ('Wet Beroepen in de individuele gezondheidszorg' or BIG Act) allows Dutch and foreign individual healthcare professionals to practice in the field of individual healthcare. The BIG Act also provides a system of 'reserved actions' ('voorbehouden handelingen') and protects the professional titles of healthcare professionals. The BIG Act provides a procedure for the cross-border recognition of professional qualifications by the recognition of foreign diplomas. Furthermore, according to Article 40 of the BIG Act, individual healthcare professionals are obliged to deliver responsible healthcare ('verantwoorde zorg').

Healthcare institutions also have the obligation to deliver responsible healthcare. This obligation is regulated in Article 2 of the Quality of Healthcare Institutions Act ('Kwaliteitswet zorginstellingen' or Kwz). Healthcare institutions must deliver responsible healthcare and must have an appropriate organization.

In 2007, the Royal Dutch Medical Association (KNMG) published a revised version of the Directive Online Doctor–Patient Contact. The Directive deals with the conditions for doctors for online communication with patients. The Directive applies to three kinds of communications:

- The doctor provides a tailored consult
- The doctor starts pharmacotherapy
- The doctor prescribes a follow-up prescription

[69] See the overview of legislation on: http://www.igz.nl/fabloket/fablok_medische_hulpmidd/med-hulpm_wetgeving. Latest update: 11 August 2009.

In the interest of the quality and continuity of healthcare, doctors must act carefully in online communications with patients. An online medical consult should be embedded in the existing medical treatment relationship between the doctor and the patient. In the absence of such a relationship, online communication is only allowed when the risks have been minimized and when the communication is in the patient's interest. From this perspective, we think, for example, that a medical twitter service like 'Tweetspreekuur'[70] needs more information than the patient can provide in a twitter message.

Furthermore, medication can only be prescribed online when a contract for medical treatment between the doctor and the patient already exists. As a result, the doctor knows the patient, has seen him before, and is in the possession of the patient's medical history. The doctor also has a reliable medical record of the patient. As from July 2007, this restriction also results from Article 67 of the Medicines Act ('Geneesmiddelenwet'), which also prohibits the prescription of medications over the internet to patients whom the prescribing doctor has never met in person, or whom the doctor does not know or of whom the doctor has no medical history available (see also, Eijpe 2008).

A doctor who offers his services on the internet also has to comply with the legal obligation to provide general information, according to Article 3:15d Civil Code (introduced by the Electronic Commerce Adaptation Act).

16.5 Conclusion

Although there is no specific Dutch legislation on eHealth, we can conclude that there is a basic legal framework in the Netherlands for eHealth scattered over different laws in both civil and public law.

At first sight, a general law on eHealth, covering all the legal aspects of eHealth might be appealing. However, the wide range of eHealth tools, from electronic patients' records to telemonitoring devices, makes a general law on eHealth difficult to achieve. Instead, the different stakeholders and supervisors, like the Healthcare Insurance Board (CVZ), the Healthcare Inspectorate (IGZ), the Healthcare Authority (NZA), and Data Protection Authority (CBP) mentioned in the scattered laws could and should think of a clear vision and policy on eHealth tools within their policy area.

The quality of healthcare is an open end. The Health Care Inspectorate enforces the quality of healthcare. Good quality of healthcare is defined in legislation (BIG, Kwz) by 'responsible care.' For an important part, the content of what is considered to be responsible care is provided by the medical professional standard that is determined by the medical professional organizations. As a result, the pallet of eHealth shows a great number of stakeholders, each with their own area of

[70] See: http://twitter.com/tweetspreekuur. Accessed 11 November 2009.

competence and with their own interest. This raises the question whether it would be beneficial to designate an organization or platform, that can at least keep an overview of the different eHealth policies from different perspectives and can initiate stakeholders to coordinate and attune policies, if necessary.

The development of clear eHealth policies by the Dutch legal supervisors and stakeholders, could be an important step to provide legal clarity, and improve the development and wider use of eHealth. But is that enough?

As mentioned many times in this chapter, eHealth by its character can make patients and healthcare providers cross national borders easily. Issues on interoperability of information and communication services, and issues of 'legal interoperability' are paramount in eHealth. These issues can best be addressed at EU level. The EU already does so. The different communications on eHealth and the proposed directive on patients' rights in cross-border healthcare are already important steps. However, the EU will have to keep on addressing those issues. From this perspective it seems regrettable that the network of the national competent authorities for eHealth, as provided in the text of the directive as accepted by the European Parliament in second reading, is only voluntary.

In the aging society where chronic diseases are increasing, eHealth has the potential to further improve the quality of healthcare and the quality of life. Of course in order to achieve that, eHealth applications will have to meet technical and legal standards. Moreover, the use of eHealth directly impacts the life and health of patients, and the work of doctors and other healthcare providers, by providing better care at lower costs. The growing participation of those two important stakeholders in eHealth, when further developing technical possibilities as well as a legal and policy framework, could really improve the trust in and the use of eHealth.

References

Callens S (2009) Legal Basis of eHealth and telemedicine. The European Files, 17

CALLIOPE (2009) Creating a European coordination network for eHealth interoperability implementation. Project Factsheet, January 2009. http://ec.europa.eu/information_society/activities/health/docs/cip/200901calliope_factsheet.pdf

Commission of the European Communities (2006) Communication from the Commission, Implementing the Community Lisbon Program: Social services of general interest in the European Union. Brussels, 26.4.2006 COM (2006) 177 final

Commission of the European Communities (2007a) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Accompanying the Communication on 'A single market for 21st century Europe' Services of general interest, including social services of general interest: a new European commitment. Brussels, 20.11.2007. COM (2007) 725 final, p 3

Commission of the European Communities (2007b) Commission Staff Working Document, Annex I to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, a lead market initiative for Europe (COM (2007) 860 final SEC (2007) 1730). Action Plan for eHealth. Brussels, 21.12.2007. SEC (2007) 1729 http://ec.europa.eu/enterprise/policies/innovation/files/leard-market-initiative/1ehealth_en.pdf

Commission of the European Communities (2008a) Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282). Off J Eur Un, 18.07.2008, L 190/37–43. 2008/594/EC

Commission of the European Communities (2008b) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Preparing Europe's digital future, i2010 Mid-Term Review. Brussels, 17.04.2008. COM (2008) 199 final http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:EN:PDF

Commission of the European Communities (2008c) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society. Brussels, 4.11.2008. COM (2008) 689 final http://ec.europa.eu/information_society/activities/health/docs/policy/telemedicine/telemedicine-com(2008)689-en.pdf

Council of the European Union (2009) Presidency compromise proposal, 31 July 2009, 12532/09

Eijpe L (2008) Study on Legal Framework of Interoperable eHealth in Europe. National Profile The Netherlands. Brussels: European Commission Directorate General Information Society. SMART 2007/0059. Issued on 30/09/2008. See also: http://www.minvws.nl/en/themes/health-insurance-system/default.asp

epSOS (2008) eHealth initiative to support medical assistance while traveling and living abroad. Project Factsheet, October 2008 http://ec.europa.eu/information_society/activities/health/docs/cip/200810epsos-factsheet.pdf

Esch RE van (2004) De Aanpassingswet elektronische handel. Computerrecht 17

European Commission (2008a) Legally eHealth, putting eHealth in its European legal context. Information Society and Media, study report March 2008

European Commission (2008b) Information Society and Media, eHealth Policy and Research Factsheet. October 2008 http://ec.europa.eu/information_society/doc/factsheets/009-ehealth-en.pdf

European Commission (2008c) Citizen's Summary: better health treatment for travelers and expats in the EU: Commission Recommendation on cross-border interoperability of electronic health record systems (2008) http://ec.europa.eu/information_society/activities/health/policy/interoperability/index_en.htm

European Commission (2009) Information Society and Media, Good eHealth Report, January 2009, p. 38. European Commission, Information Society and Media, Good eHealth. Exchange of Good Practices on eHealth—Knowledge Base http://www.good-ehealth.org/

Gronden JW van de, Sluijs JJM (2009) De betekenis van het EG-Verdrag voor het reguleren van de zorgmarkt. Preliminary Advice for the Dutch Health Law Association

Hooghiemstra T, Nouwt S (2007) Tekst en toelichting Wet bescherming persoonsgegevens. SDU Uitgevers (derde herziene druk), Den Haag

I.COM Innovation Centre of Mental Health & Technology, E-mental health: presence and future. Factsheet e-Mental Health. http://www.icom.trimbos.nl/documents/downloads/factsheet%20e-mental%20health%20(I.COM).pdf

Jong C de, Kunst G (2005) 'Shared Values', Onderzoek stand van zaken en ontwikkeling van Domotica in de zorg. 29 April 2005, p 5 http://www.bouwcollege.nl/Pdf/Ontwerpaspecten/domotica%20onderzoek.pdf

Ministry of Health, Welfare and Sport (2006) ICT in Dutch Healthcare: an International Perspective. May 2006

Sander C (2001) Consumentenbescherming bij transacties op afstand. SDU Uitgevers, Den Haag

Swedish Presidency of the European Union, Health Care Division (2009) Activity Plan on eHealth during the Swedish Presidency of the EU. 5 July 2009, revised. The Presidency report eHealth for a Healthier Europe is available at: http://www.se2009.eu/polopoly_fs/1.8225.1247835182!menu/standard/file/eHealth%20for%20a%20Healthier%20Europe.pdf

The Prague Declaration (2009) eHealth for Individuals, Society and Economy. 20 February 2009: eHealth 2009 Conference Declaration http://www.ehealth2009.cz/

Chapter 17
Implementation of the EU Services Directive: On eGovernment in a Decentralized Unitary State

Astrid M. M. van der Wijst and Marga M. Groothuis

Abbreviations

IMI Internal Market Information System
GALA General Administrative Law Act

Contents

17.1 Introduction 316
17.2 Point of Single Contact—Legal and Organizational Framework 317
17.2.1 Basis of EU Law 317
17.2.2 Legal and Organizational Implementation in the Netherlands 317
17.3 Challenges from a Constitutional Point of View 319
17.4 Legal Assessment: Principles of Good Governance Applied in a Digital Context 321
17.5 Conclusion 325
References 326

Contribution received in 2010.

A. M. M. van der Wijst
The Environmental Protection Agency, West-Holland, The Netherlands

M. M. Groothuis (✉)
The Institute for Public Law at Leiden University, Leiden, The Netherlands
e-mail: m.m.groothuis@law.leidenuniv.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_17,

17.1 Introduction

The EU Services Directive, which came into force on December 28, 2006 and set an implementation deadline for December 28, 2009, has had a major impact on eGovernment practices in the 27 EU Member States.[1] Article 8 of the Services Directive establishes an obligation for Member States to "ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant Point of Single Contact and with the relevant competent authorities." Electronic means have to be available for the whole administrative process, from the service provider's initial application and submission of documents to the final reply by the relevant competent authority.

In order to implement this European norm, each of the 27 EU Member States has, in the period 2007–2009, set up a national electronic desk—Points of Single Contact—through which service providers (e.g., accountants) from other EU Member States can complete legal procedures by electronic means and at a distance (e.g., the procedures to be followed by a French accountancy firm to obtain permits for a new office it intends to open in Amsterdam).

The aim of this chapter is twofold. First, it seeks to analyze the impact of the EU Services Directive on the legal framework for eGovernment in the Netherlands, an EU Member State which can be characterized as a "decentralized unitary state." Second, it aims to discuss the legal and technological factors which demand special attention when building an institutional framework for national eGovernment services in a decentralized unitary state.

The outline is as follows. Section 17.2 briefly describes the legal and organizational framework for the new electronic Point of Single Contact in the Netherlands. Section 17.3 investigates the extent to which the concept of "Point of Single Contact" fits into the constitutional framework of a decentralized unitary state like the Netherlands. How does the EU goal of one Point of Single Contact within each EU Member State relate to the Dutch Constitution and basic laws, with their emphasis on a distribution of powers among several levels (national level, provinces, and municipalities)? Further, Sect. 17.4 provides a legal assessment of the Point of Single Contact under the general principles of good governance, such as legality, reliability, and confidentiality. Finally, Sect. 17.5 draws conclusions on the question of which legal and technological factors need to be taken into account when building an institutional framework for national eGovernment services in a decentralized unitary state.

[1] See for an introduction to the EU Services Directive and its implementation in the EU Member States: Barnard 2008, pp. 323–394; De Waele 2009, pp. 523–531.

17.2 Point of Single Contact—Legal and Organizational Framework

17.2.1 Basis of EU Law

The legal basis of the electronic Point of Single Contact in the Netherlands is constituted of Articles 6, 7, and 8 of the EU Services Directive. On the basis of Article 6, Member States are obliged to ensure that service providers can complete all procedures and formalities needed for access to and exercise of their service activities through "Points of Single Contact". These points are meant to be the single institutional interlocutors from the perspective of the service provider, so that he does not need to contact several competent authorities or bodies to collect all relevant information and to complete all necessary steps relating to his service activities. Article 7(1) contains a list of essential information which Member States must make easily accessible through the "Points of Single Contact" to service providers and service recipients. This information needs to be accessible at a distance and by electronic means.

Furthermore, Article 8, as cited above (Sect. 17.1), establishes an obligation for Member States to ensure that all procedures and formalities may be easily completed, at a distance and by electronic means. Procedures and formalities which service providers need to be able to complete by electronic means, in principle, encompass all procedures and formalities relating to access to a service activity, and to the exercise thereof.[2]

Finally, Article 34 prescribes that the Member States, in cooperation with the European Commission, shall establish an electronic system for the exchange of information between Member States (the IMI: Internal Market Information System).

17.2.2 Legal and Organizational Implementation in the Netherlands

The legislative implementation of these provisions of EU law in the Netherlands has been realized in two steps: the Services Act ("Dienstenwet")[3] and an

[2] Art. 8(2) contains three exceptions from the obligation to provide for electronic means: (i) the inspection of premises on which the service is provided; (ii) the inspection of the equipment used by the provider; and (iii) the physical examination of the capability or the personal integrity of the provider or his staff.

[3] Complete title: "Wet van 12 November 2009 tot implementatie van Europese regelgeving betreffende het verkeer van Diensten op de interne markt (Dienstenwet)," adopted in the Senate on November 10, 2009, Kamerstukken I (First Chamber of Parliament) 2008/09, 31579, A.

Adaptation Act.[4] The Services Act addresses, inter alia, the measures prescribed by Article 8 of the Services Directive. Furthermore, it offers the legal framework for the Dutch Point of Single Contact and the IMI system.[5] On December 28, 2009, the Services Act and the Adaptation Act entered into force.[6]

According to Articles 5 and 13 of the Services Act, the Dutch Minister of Economic Affairs is responsible for the establishment, maintenance, and security of the Point of Single Contact. Furthermore, he has the legal duty to ensure service providers and government agencies exchange information with each other, and perform legal procedures and formalities, via this electronic central desk.

In practice, the Dutch Point of Single Contact has been set up as follows.[7] The Ministry of Economic Affairs has created a digital environment, secured by—inter alia—a Secured Socket Layer (SSL), which can be reached via a central website, named Message Box. This digital environment consists of two sections: (1) a section for mailboxes for service providers (e.g., a French accountancy firm that wishes to apply for a permit to open a new office in Amsterdam) and (2) a section for mailboxes for competent authorities (e.g., the Mayor and Aldermen of Amsterdam who are competent to decide on building permits in that city).

After digital registration, a service provider receives a user name and password which enables him to log into the secured digital environment and create his own (personal) message box. Via this mailbox, he can communicate, and perform legal procedures with, all Dutch government agencies that fall under the scope of the EU Services Directive. Examples of legal procedures and formalities which can be performed via Message Box are applications for inclusion in the Dutch Accountants' Register (as in the example mentioned above), inclusion in the Trade Register and occupancy permit and notification of occupancy.[8] In his personal, secured, message box, a service provider can draft and send messages (e.g., letters), fill in and submit application forms (which can be downloaded on other web pages provided by Dutch government agencies), receive and read incoming messages, including formal decisions by government agencies, forward received messages to other mailboxes, and delete messages. Thus, the Message Box (or, in the terminology of the EU Law directive, Point of Single Contact)

[4] Published in Staatsblad (Publication Journal) 2009, 616. See for the explanatory memorandum of this Act: Kamerstukken II (Second Chamber of Parliament) 2008/09, 31 859, No. 3. This Act provides for amendment of sector-specific legislation.

[5] These aspects of the Services Act will be analyzed below, in Sects. 17.3 and 17.4.

[6] Publication of the Services Act: Staatsblad (Publication Journal) 2009, 503 (adopted text) and Staatsblad 2009, 505 (date of entering into force).

[7] This description is based on: the Explanatory Memorandum to the Services Act, Kamerstukken II, 2008/09, 31 579, nr. 3, the Explanatory Memorandum to the "Dienstenbesluit Centraal Loket" (a Governmental Degree based on the Services Act, Staatsblad 2009, 504, and the website www.answersforbusiness.nl (website set up by the Dutch Ministry of Economic Affairs for entrepreneurs).

[8] An overview of proceedings that can be performed digitally via the Message Box can be found at http://www.answersforbusiness.nl/messagebox/procedures. This overview is not yet complete and will be further expanded.

constitutes a "digital switch" between the service provider and the government agency.

The technical requirements and organizational aspects for the Message Box, and the competences of the Minister related to it, are laid down in the "Dienstenbesluit centraal loket" (a Governmental Degree)[9] and the "Dienstenregeling centraal loket en interne markt informatiesysteem" (a Ministerial Regulation).[10] These include provisions on data security, requirements of confidentiality, as well as rules on the reliability of the information system (requirements of integrity).

17.3 Challenges from a Constitutional Point of View

Since the early stages of the parliamentary debate on the Dutch Services Act, there has been attention on challenges from a constitutional point of view. It has been argued that there is a tension between, on one hand, the principle of respect for the allocation, under Dutch constitutional law, of functions among relevant competent authorities at the national, regional, and local level, and on the other hand, the creation of the digital "Point of Single Contact" as required by Articles 7 and 8 of the EU Services Directive. In this section, we first analyze the cause of this tension. Further, we investigate the extent to which the EU-concept of a "Point of Single Contact" fits into the constitutional and legal framework of the Netherlands.

An essential characteristic of a decentralized unitary state like the Netherlands is that the Constitution allocates legislative and executive powers to authorities at different levels of the state: national level, regional level (provinces), and local level (municipalities).[11] In this context, Dutch constitutional law distinguishes between autonomous powers ("autonomie") and shared powers ("medebewind") (Kortmann and Bovend'Eert 2007, p. 43). Regarding the first category, Article 124 of the Constitution provides that the powers to regulate and administer their own affairs shall be left to the decentralized authorities. This means that, except where there are statutory provisions to the contrary, the provincial states and municipal council possess the full range of regulatory and administrative powers. Only if these powers have been allocated to other authorities by Act of Parliament, or by

[9] Degree of November 26, 2009 ("Besluit houdende regels ter uitvoering van de Dienstenwet met betrekking tot het centraal loket," "Dienstenbesluit centraal loket"), published in Staatsblad 2009, 504.

[10] Regulation of the Minister of Economic Affairs of November 27, 2009 (No. WJZ/9214712, "Dienstenregeling centraal loket en interne markt informatiesysteem"), published in Staatscourant (Publication Journal) 2009, 18558.

[11] The Dutch Constitution also attributes legislative and administrative powers to Water Boards ("Waterschappen"), which have a general, regulatory, and administrative role within their territorial boundaries for matters which fall within the scope of the "waterstaat," i.e., water management: Kortmann and Bovend'Eert 2000, p. 54.

bye-laws ("verordeningen") issued by the local authority itself pursuant to an Act of Parliament, is this otherwise (Kortmann and Bovend'Eert 2007, p. 48).[12]

This feature of decentralization in the Dutch Constitution seem to impinge on the requirement, based on Article 8 of the EU Services Directive, to ensure "that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant Point of Single Contact and with the relevant competent authorities." This provision of European law implies an element of centralization.

In this context, another Act is also relevant: the General Administrative Law Act (GALA) ("Algemene wet bestuursrecht").[13] This Act contains a section on electronic communication between government agencies and citizens (Section 2.3).[14] It regulates under which conditions electronic communication with government agencies is allowed. Two principles are central here. The first principle is that electronic communication is allowed if both the government organization and the citizen(s) involved, agree to permit it. Citizens or entrepreneurs are not obliged to communicate electronically with government agencies (Art. 2:14 GALA). On the other hand, they have no right to do so if the government agency chooses not to use electronic means of communication (Art. 2:15 GALA). The second principle is that the electronic message meets requirements of reliability and confidentiality: an electronic message may only be sent if the electronic system is sufficiently reliable and confidential, given the nature of the communication.

In the academic debate on the implementation of the EU Services Directive in the Netherlands, it was argued that the introduction of a digital Point of Single Contact (Arts. 6–8 of the EU Directive) would require amendments of the General Administrative Law Act. Several authors (Widdershoven et al. 2007, p. 97; Duijkersloot and Widdershoven 2007, pp. 196–200; Belhadj et al. 2007, p. 149) stated, referring to case law of the European Court of Justice,[15] that Article 2:15 GALA was incompatible with Article 8 of the EU Services Directive and would need to be amended.

An Advisory Committee to the National Government, the Commissie Evaluatie AWB III, took a different view. According to this Committee the (only) requirement prescribed by the EU Services Directive was that the EU service providers be

[12] More detailed regulations on the powers of the states and council have been laid down in the Provinces Act and the Municipalities Act (Prakke and Kortmann 2004, p. 638). These Acts contain the basic provision concerning the autonomous authority to issue bye-laws: it states that the provincial state and the municipal council issue bye-laws which they consider to be in the interest of the Province or Municipality.

[13] A translated version, in English, of this act is available on the website of the Dutch national government: http://www.rijksoverheid.nl/onderwerpen/algemene-wet-bestuursrecht-awb.

[14] Arts. 2:13–2:17 GALA.

[15] Case law on principles of EU law with regard to implementation of EU directives into national legislation (inter alia, the principle of loyal cooperation and the requirement of consistent interpretation): European Court of Justice May 10, 2001, C-144/99 (*European Commission* v. *the Netherlands*); European Court of Justice July 12, 2007, C-507/04 (*European Commission* v. *Austria*).

able to complete proceedings and formalities digitally; this requirement would, however, not have to be laid down in legislation (Commissie Evaluatie AWB III 2007, p. 55).

The Dutch legislator did not agree to this. A Bill was prepared[16] and adopted[17] in 2009 which—inter alia—contains deviations from Articles 2:14 and 2:15 GALA.[18] Under the new legislation, government agencies no longer have the power to refuse to communicate electronically with EU service providers. Each government agency, at the national, provincial or local level, is required to connect to the national Point of Single Contact (Message Box), and set up and maintain an organizational and technological framework for processing all proceedings and formalities relating to EU service providers via this digital channel, as well as participate in the IMI.[19] The new legislation was adopted only recently (in December 2009) and its effects have not yet been evaluated. It is expected, however, that it will substantially strengthen the ongoing efforts[20] to work toward interoperable eGovernment services for businesses in the Netherlands (Steyger 2008, pp. 9–10; Backes 2009, pp. 316–317).

17.4 Legal Assessment: Principles of Good Governance Applied in a Digital Context

In this section, we investigate which legal and technological factors demand special attention when building an institutional framework for national eGovernment services in a decentralized unitary state. In our view, three principles of good governance ("beginselen van behoorlijk bestuur"), developed in Dutch literature and case law (Nicolaï 1990; Franken 1993; Addink 1999) are particularly relevant in this context: the principles of legality, reliability, and confidentiality. The legality principle requires government action to have a foundation in formal law.

[16] Proposal for the Services Act ("Dienstenwet"), Kamerstukken II 2007/08, 31 579, Nos. 1–3.

[17] First Chamber of Parliament, November 10, 2009, Handelingen Eerste Kamer 2008/09, EK-8, pages 8–822 until 8–240.

[18] A detailed description of these deviations and analyses of their consequences for eGovernment under the Dutch system of administrative law can be found in: Backes 2009, pp. 307–317; Duijkersloot and Widdershoven 2007, pp. 190–204; Hessel 2007, pp. 113–125.

[19] See for a description and analysis of the policies developed by the Dutch Ministers of Economic Affairs, and Interior Affairs, and Kingdom Relations and the decentralized authorities in order to meet with these requirements: van Meerten 2008, pp. 1–37. See furthermore the letters (in Dutch) of the Minister of Economic Affairs to the Second Chamber of Parliament of December 13, 2007 (Kamerstukken II 2007/08, 21501-30 and 31200 XIII, No. 172) and March 19, 2008 (Kamerstukken II 2007/08, 21 501-30, No. 178).

[20] An overview of these measures, implemented in the years 2008–2010, is given in a letter (in Dutch) of the Deputy Minister of Interior Affairs and Kingdom Relations "Modernisering van de overheid" to the Second Chamber of Parliament of December 18, 2009 Kamerstukken II 2009/10, 29 362, nr. 157, pp. 1–21, and four attachments (policy reports) to it.

The principles of reliability and confidentiality refer to a set of five "benchmarks" for electronic communication and processing of information in public administration: accessibility, authenticity, reliability, integrity, and transparence (Franken 1993, pp. 18–22; Groothuis 2004, pp. 19–23).

When applying these principles to the digital Point of Single Contact, five aspects have turned out to be particularly challenging from a legal point of view.

First, the principle of legality requires a legal basis (new legislation) for the Point of Single Contact and the cooperation between various administrative authorities in its context. The basic legal framework, the Services Act and Adaptation Act, has entered into force in December 2009 (as described in Sect. 17.2 of this chapter). A major challenge, however, will be to further integrate the new Point of Single Contact and the IMI into the already existing legal and organizational framework for eGovernment (van Meerten 2008, pp. 31–32).

In the period of 2005–2010, eGovernment policies in the Netherlands focused on the reduction of administrative burdens for business and citizens, and on improving the effectiveness of the working processes within government organizations.[21] Therefore, priority has been given to the restructuring of the data administration within the entire administration—both central and decentralized—through the development and introduction of a basic data registration ("Basisadministraties") and identification numbers for business and citizens (van Meerten 2008, p. 31). Besides the existing registration (persons, trade register, and land register) six new registrations were developed—buildings and addresses, vehicles, wages, employment and benefit relationships, income, and real estate value.

Maintaining these basic registrations is a task allocated to the administrative authorities at both the central and the decentralized levels of the state. These authorities have also been allocated, under the Services Act, the task of connecting to the Point of Single Contact, and exchanging information and cooperating with (central and decentralized) authorities of other EU Member States via the IMI. Connecting, integrating, and maintaining these technological frameworks has required and will continue to require additional, complex legislation, especially because of the necessity of the reallocation of competences among various authorities at the central and decentralized levels of government (van Meerten 2008, p. 32).

Second, in the context of the cross-border cooperation and exchange of information between competent authorities via IMI, the requirement of reliability plays an important role. If the data sent to, or received from authorities in other Member States, are not reliable (i.e., incorrect) or misinterpreted, serious negative effects for the involved service providers can occur. The Services Directive does not regulate this situation. Drawing from Steyger (2008, p. 9), however, we argue that it follows from the principle of community loyalty (Art. 4, Section 3 TEU) that fast and effective administrative proceedings must be available to service providers

[21] The legal and technological framework for this policy is described in: Kamerstukken II 2007/08, 29 362, Nos. 120, 124, and 125 (Government Modernization).

which enable them to report errors or misinterpretations in data exchanged via IMI and to submit requests for correction.

Third, the requirement of accessibility of the Point of Single Contact deserves special attention. By that, we do not only mean accessibility in technological terms (e.g., which software can, or cannot, be used by service providers, to download or submit a form via the Point of Single Contact). We also mean accessibility with regard to language. The Services Directive does not prescribe that information on the Points of Contact is made available in more than one language (e.g., Dutch and English). Article 7(5) of the Services Directive merely establishes that the use of more than one language is "encouraged". If, however, the information and digital forms available on the Point are not in a language that service providers know (e.g., English), there will—in practice—be a substantial barrier for the service provider to use the Point as a channel for communication.[22]

Fourth, Article 2:15, Section 3 of the General Administrative Law Act, establishes that an administrative authority may refuse to accept a communication sent electronically if the reliability or confidentiality of the communication is not sufficiently safeguarded, with regard to the nature and content of the communication and the purpose for which it is used. These rules also apply when the communication is sent via the Point of Single Contact. Both the criteria of reliability and confidentiality depend on the state-of-the-art (van der Hof 2007, p. 9).

The competent authorities, e.g., the Mayor and Aldermen of a municipality in proceedings for a building permit, are responsible for the reliability and confidentiality of the communication. This follows from the system of the GALA and the Services Act. Reallocating the competence to refuse a communication to the Minister of Economic Affairs, who is responsible for the Point of Single Contact, would have been incompatible with the constitutional autonomy of the provinces and municipalities. Thus, the Minister would interfere too much into the affairs of the decentralized authorities.[23]

The fact that the competence to refuse a communication, and to establish the required levels of reliability (and confidentiality), lies with each competent authority, means that in practice hundreds of government agencies at the central and decentralized level of government in the Netherlands can determine their own "standards" for refusing messages sent to them by service providers. This could lead to much variety in policy between government agencies and thus potentially

[22] The Commission emphasizes the importance of the availability, on the Points of Single Contact of all Member States, of information in more than one language. More concretely, it recommends making information available in languages of the neighbouring Member States and "in languages most commonly used by businesses in the EU": European Commission 2007, p. 21.

[23] This view (on the autonomy of the municipality with regard to its communication) was confirmed in the debate on the Services Act in the First Chamber of Parliament on 10 November 2009: Handelingen I 2008/09, EK-8, 8-222 and 8-229. See also Art. 2, sub b, of the Services Degree (discussed above in Sect. 17.2 of this chapter), which establishes that the Point of Single Contact must enable the competent authority to take its own (additional) measures with regard to reliability and confidentiality.

undermine the concept of a Point of Single Contact. However, the principle of community loyalty (Art. 4, Section 3, TEU) implies in our view that a competent authority, when considering to refuse an incoming electronic message from a service provider, should balance on one hand the interest of safe communication and reliability of its (own) information system and on the other hand the interest of the service provider to be able to perform formalities and proceedings electronically.

Fifth, establishing the authenticity of electronic communication has been a challenging aspect of the Point of Single Contact. Article 2:16 GALA regulates the electronic signature. It states that an electronic signature satisfies the requirement of signature if a sufficiently reliable authentification method is used, with regard to the nature and content of the electronic communication and the purpose for which it is used. Paragraphs 2–6 of Articles 15a and 15b of Book 3 of the Civil Code apply mutatis mutandis where this is not incompatible with the nature of the communication. These provisions of the Civil Code implement Directive 99/93/EC of the European Parliament and of the Council of December 13, 1999 on a Community framework for electronic signatures, are based on a functional approach as well as on the distinction between advanced and normal e-signatures as laid down in the Directive. These provisions are applicable to government e-communications, unless the nature of the message concerned opposes such an application (van der Hof 2007, pp. 9–10).

An electronic signature is requested under Dutch law[24] for, inter alia, applications for permits, grants, subsidies, and other decisions in individual cases ("beschikkingen"). This means, in practice, that every application form submitted via the Point of Single Contact by a service provider (e.g., the application form submitted by a Greek transport company for inclusion in the Trade Register in Rotterdam) must be signed by means of an electronic signature which meets the requirements of Article 2:16 GALA.

Two aspects are problematic in this context. One is that each competent authority can determine, under Article 2:16 GALA, which means of identification and authentification can be used for a particular formality or proceeding. For example, the Mayors and Aldermen of each of the 418 municipalities in the Netherlands can prescribe, under Article 2:16, which type of electronic signature may be used by service providers (from all EU Member States) to submit an application for a building permit. The Minister of Economic Affairs, who is competent for the maintenance of the Point of Single Contact, cannot prescribe that only one type of electronic signature be prescribed for a particular formality, in all municipalities, or in all provinces.[25] As a result, it may be very difficult for a service provider from any of the 27 EU Member States to complete formalities and proceedings electronically, via the Point of Single Contact, when competent authorities in each of the 430 municipalities, 12 provinces, and at the national level

[24] Art. 4:1 GALA.

[25] See also: Kamerstukken II 2007/08, 31 579, No. 3, p. 38.

can, within the framework of Article 2:16 GALA, set their own standards for authentification.

A second, related, problem is the limited cross-border interoperability[26] of the authentification methods. In November 2008, the Commission published an "Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market."[27] The objective of this Action Plan is to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures and e-identification, which will simplify access of enterprises and citizens to cross-border electronic public services. To achieve this objective, the Action Plan focuses on a number of practical, organizational, and technical issues, complementing the existing legal framework.

On October 16, 2009, a first legislative measure was taken: the Commission published a Decision[28] aimed at improving the cross-border interoperability of electronic signatures. Article 1, para 3, of this Decision states that "Member States shall not make the acceptance of advanced electronic signatures based on a qualified certificate, with or without a secure-signature-creation device, subject to requirements which create obstacles to the use, by service providers, of procedures by electronic means through the points of single contact."[29] This means—in short—that competent authorities must accept all electronic signatures which offer a higher level of reliability and confidentiality than the electronic signatures prescribed by themselves. This new provision offers a legal–technical short-term solution but does not envisage a substantive long-term strategy. In our view, a modernization of the Electronic Signatures Directive is necessary in order to achieve genuine cross-border interoperability of eGovernment services for business.

17.5 Conclusion

The goal of this chapter was twofold: (1) to investigate the impact of the implementation of the Services Directive on the previously existing framework for eGovernment in the Netherlands and (2) to investigate which legal and

[26] Interoperability can be defined as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" (Snellen and Thaens 2008, p. 28).

[27] Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM (2008) 798 final, Brussels, November 28, 2008.

[28] Commission Decision of October 16, 2009 setting out measures facilitating the use of procedures by electronic means through the Points of Single Contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market [notified under document C(2009) 7806]. A Corrigendum to this Decision was published in OJ*EU* L299/18, November 14, 2009.

[29] See on the implementation of this Commission Decision into Dutch law (Adaptation Act): Kamerstukken I 2008/09, 31 579, C. p. 36 and Kamerstukken II 2008/09, 31 859, No. 4.

technological factors demand special attention when building an institutional framework for national, centralized eGovernment services in a decentralized unitary state.

We conclude, first, that the implementation of the Services Directive has the potential of strengthening the already ongoing efforts to work toward interoperable eGovernment services for businesses. A boost has been created, in particular, by the introduction into Dutch law of the rule that all procedures and formalities may be completed at a distance and by electronic means. This constitutes a significant turning point in the Netherlands, where until recently competent authorities were encouraged, but not forced to offer electronic procedures to business and citizens. At the same time we find that there remains a tension between, on one hand, the principle of respect for the allocation, under Dutch constitutional law, of functions among relevant competent authorities at the national, regional and local level, and on the other hand the creation of the Point of Single Contact. This tension can be observed in particular with regard to the remaining power of regional and local authorities to set their own requirements for the authentification of electronic documents.

Furthermore, we conclude that three principles for public governance developed in European and Dutch case law and legislation—the principles of legality, reliability, and confidentiality—constitute useful benchmarks for building an institutional framework for national eGovernment services in a decentralized unitary state.

Finally, we have found that the requirements for the electronic signature and the limited level of cross-border interoperability of the chosen authentification methods create a major challenge for the competent authorities and other involved parties. A recent report of the European Commission indicates that this problem is not uniquely Dutch, but part of a much wider European problem of limited interoperability of authentification methods, not only with regard to procedures and formalities for service providers, but also for businessmen and citizens alike. A Commission Decision published in October 2009 offers a legal–technical short-term solution but does not envisage a substantive long-term solution. In our view, a modernization of the Electronic Signatures Directive is necessary in order to achieve genuine cross-border interoperability of eGovernment services for business.

References

Addink GH (1999) Algemene beginselen van behoorlijk bestuur. Kluwer, Deventer

Backes ChW (2009) Much ado about nothing of het begin van een nieuwe bestuurscultuur? De omzetting van een nieuwe bestuurscultuur? De omzetting van de Dienstenrichtlijn. Nederlands Tijdschrift voor Bestuursrecht, pp 307–317

Barnard C (2008) Unravelling the services directive. Common Mark Law Rev 45:323–394

Belhadj E, Evans SJH, van de Gronden JW (2007) de Dienstenrichtlijn; de gebreken van de deugden? Een eerste verkenning van de Dienstenrichtlijn, SEW. Tijdschrift voor Europees en Economisch Recht, pp 141–153

Commissie Evaluatie AWB III (2007) Toepassing en effecten van de Algemene wet bestuursrecht 2002–2006. WODC, Boom Juridische Uitgevers 2007, The Hague
De Waele H (2009) The transposition and enforcement of the services directive: a challenge for the European and national legal orders. Eur Pub Law 15(4):523–531
Duijkersloot APW, Widdershoven RJGM (2007) De Dienstenrichtlijn en het algemeen bestuursrecht. RegelMaat, aflevering 5:190–204
European Commission (2007) Handbook on implementation of the services directive, Brussels 2007. http://ec.europa.eu/internal_market/services/services-dir/index_en.htm
Franken H (1993) Beschikken en automatiseren, Kanttekeningen bij het automatiseren van beschikkingen advisory report for the Dutch association for administrative law. Alphen a/d Rijn, Samsom
Groothuis MM (2004) Beschikken en digitaliseren, over normering van de elektronische overheid. SDU, The Hague
Hessel B (2007) Gemeenten en de dienstenrichtlijn (1). Gemeentestem 7269:113–125
Kortmann CAJM, Bovend'Eert PPT (2000) Dutch constitutional law. Kluwer Law International, The Hague
Kortmann CAJM, Bovend'Eert PPT (2007) Constitutional law of the Netherlands. An introduction. Kluwer, Alphen an den Rijn
Nicolaï P (1990) Beginselen van behoorlijk bestuur. Kluwer Law International, Deventer
Prakke L, Kortmann C (eds) (2004) Constitutional law of 15 EU member states. Kluwer, Deventer
Snellen ITM, Thaens M (2008) From e-Government to m-Government. Towards a new paradigm in public administration? In: Pennella G et al (eds) Administrative innovation, international context and growth. Formez, Gianni Research 2008, pp 1–33
Steyger E (2008) De implementatie van de Dienstenrichtlijn en het algemeen bestuursrecht. Nederlands Tijdschrift voor Bestuursrecht, pp 1–10
Van der Hof S (2007) The status of eGovernment in the Netherlands. Electron J Comp Law 11:1–18. http://www.ejcl.org/111/art111-13.pdf
Van Meerten H (2008) National report of the Netherlands on the new services directive. Report for FIDE 2008, XXIII, Congress, Linz, pp 1–37
Widdershoven RJGM et al (2007) De Europese agenda van de Awb. Boom Juridische Uitgevers, The Hague

Chapter 18
The Impact of Europe on Geo-Information

Leo van der Wees

Abbreviations

GIS Geographical information system
PSI Public sector information

Contents

18.1 Introduction 330
18.2 What is Geo-Information? 331
18.3 European Rules in the Context of Geo-Information 332
18.3.1 Directive 96/9/EC on the Legal Protection of Databases 332
18.3.2 Directive 2003/98/EC on the Reuse of Public Sector Information 333
18.3.3 Directive 2007/2/EC Establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) 334
18.4 The Directives Evaluated: Is there an Impact on Geo-Information? 335
18.4.1 Directive 96/9/EC on the Legal Protection of Databases 335
18.4.2 Directive 2003/98/EC on the Reuse of Public Sector Information 336
18.4.3 Directive 2007/2/EC Establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) 337

Contribution received in 2010.

L. van der Wees (✉)
Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, The Netherlands
e-mail: wees@recht.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_18,

18.5 The *Landmark* Case: A Landmark Decision for Geo-Information 338
18.6 Other Initiatives to Improve Dissemination of Geo-Information in The Netherlands 340
18.7 Conclusion 341
References 343

18.1 Introduction

One of the first important documents on the disclosure of public sector information produced in The Netherlands was Towards Accessibility of Government Information ('Naar toegankelijkheid van overheidsinformatie').[1] In this memorandum, the Ministry of the Interior describes its line of policy as, increasing the accessibility of public sector information with the help of information technology. The starting point of the memorandum was the existing policy framework on the disclosure of public sector information. Two major topics were described. Firstly, to explore the possibilities of using ICTs to provide the public with information in order to enlarge citizen involvement in the democratic process. Secondly, to look into the possibilities to create new business opportunities by exploiting electronic data files containing public sector information. In relation to the first topic of the memorandum, Dutch parliamentary documents (around 1997), case law (1999), and acts (2002) were made available to the public via the Internet.

The publicly available geo-information is information which could play a role in creating new business opportunities, the second topic of the memorandum. However, in 2010 there is hardly any geo-information readily available, and as a result, no new businesses have been created. A brief description of the history of the disclosure of geo-information will clarify why.

Quite some time before the memorandum on the disclosure of public sector information was publicized, organizations started to digitize geological information. This resulted in about 25,000 geo-data sets being produced in The Netherlands at the end of the 1999 (BDO 1998). Strangely enough, this did not lead to a widespread use of digital geo-information. This was because after the geo-data was digitized, the administrators of the organizations using the material were afraid of misuse and losing control over the information, therefore, often used an 'in-house only' policy. As a result, the digital data sets were used within the organizations, but external contacts were provided with paper versions only (Zeeuw 2007).

Due to social pressure and cuts in the budgets of organizations processing geo-data, the policy was changed resulting in the availability of digital geo-data sets to others besides just the internal organization. Unfortunately, this process was started without having an overall national strategy, and therefore, did not result in

[1] Kamerstukken (Parliamentary documents) II 1996–1997, 20644, nr. 30, 'Informatievoorziening openbare sector'; Brief staatssecretaris met nota 'Naar toegankelijkheid van overheidsinformatie'.

a widespread reuse of geo-data. Organizations started applying their own use and price policies which led to a new problem: a maze of rules and conditions for the reuse of digital geo-data sets by third parties. As a matter of fact, this is still the case in The Netherlands. In general, there is hardly a uniform, clear, and transparent policy on the disclosure of geo-information in spite of the Memorandum Towards Accessibility of Government Information published in 1997. It has not led to a dissemination of geo-information comparable to the freely accessible parliamentary documents, acts, and case law.

This situation is one of missed opportunities. Links between geo-data sets for emergency services are not made easily, business opportunities are left unused, and costs to obtain geo-data are often high. Changing the status quo is not easy, due, amongst others, to the fact that part of certain public organizational activities are financed from revenues of the sale of geo-information (Loenen 2005). Nonetheless, some changes seem to be occurring in the geo-field as well. After influencing the disclosure of parliamentary and legal documents the Dutch policy described in Towards Accessibility of Government Information and subsequent policy documents on public sector information (Nouwt 2008, p. 59) after many years, also seem to get their impact on geo-information. Technical developments resulting in an easier transport, storage, and processing of geo-data play a role in this process as well, and not to forget European Union influences. Various European directives have stimulated the disclosure of geo-information as will be described below.

In this chapter, I will first describe what geo-information is (Sect. 18.2). Subsequently, I will explore the European rules which have relevance for (the dissemination of) this type of information and discuss whether or not these European rules have a de facto impact (Sect. 18.3). Also, the most important Dutch lawsuit on geo-information so far, the *Landmark* case, will be analyzed (Sect. 18.4), as well as various initiatives of the Dutch government to improve the availability of geo-information (Sect. 18.5). The chapter concludes with remarks and an agenda for further research (Sect. 18.6).

18.2 What is Geo-Information?[2]

Geo-information is an abbreviation of geographic information. It is information connected to a place on earth. This information connects a location, time, and characteristics of that particular location. The information can be related to real or virtual matters. Real are, for example, visible fixed objects, like buildings, or invisible objects, like underground cables and wires (Longley 2001, pp. 64, 65). An example of geo-information related to virtual matters, is that on borders.

Geo-information plays a role in several governmental tasks. Lots of ministries produce, use and/or exchange geo-information, and the same is true for provinces,

[2] Based on Loenen 2008.

district water boards, and municipalities. In addition, semi-governmental institutes like the Land Register and The Royal Netherlands Meteorological Institute, use, produce, and disseminate geo-information.

The processing of geo-information is often done using a geographical information system (GIS). A GIS captures, stores, analyzes, manages, and presents data that is linked to a location (Worboys 1995). A GIS can give an insight into specific characteristics of a certain location. One can think of the presence of a supermarket in a district, the average income in a specific area, or the availability of industrial properties of a certain size.

This chapter refers to geo-information of fixed locations which are processed by geographical information systems. This means information about the location of mobile devices, however, interesting, will not be discussed. It would require another chapter to do so. See Nouwt (2008) for more information on this type of geo-information.

18.3 European Rules in the Context of Geo-Information

Several European rules are important to bear in mind in a discussion on geo-information. Below the most relevant directives are shortly described in chronological order.

18.3.1 Directive 96/9/EC on the Legal Protection of Databases

The European Commission thought that with the advent of the information society, the protection of databases would become very important, given that a lot of online services would be provided via an electronic database. The idea was also that databases would have a significant impact on the creation of new multimedia products. Databases should, therefore, be given an appropriate level of protection to create an attractive environment for investment while safeguarding users interests. The result was a proposal for a Directive to protect databases.

The proposal for a Directive on the legal protection of databases was adopted in 1996. The Directive created a new exclusive 'sui generis' right for database producers and harmonized copyright law applicable to the structure and arrangement of the contents of databases.

The *sui generis* right, valid for 15 years, gives the creator of a database the right to protect the investment of time, money and effort, irrespective of whether the database in itself is innovative ('non-original' databases). A lawful user may retrieve and reuse, without authorization, non-substantial parts of the contents of a database. However, he may not perform acts that unreasonably prejudice the legitimate interests of the creator of the database, or of a person providing the works or services contained therein.

Protection against unauthorized retrieval or reuse is given to databases whose maker is a citizen, a company or an undertaking resident in or having a registered office, central administration or main place of business in the European Community.

The harmonization of copyright law applicable to databases gives the maker, protection of the database when it constitutes, by virtue of the choice or arrangement of the material, an intellectual creation ('original' databases). The creator of such a database enjoys exclusive rights.

The Directive applies to both analog and digital databases.

Neither the Directive nor its considerations pay special attention to databases containing geo-information. This of course does not mean this Directive cannot and will not play a role in the field of geo-information. The *Landmark* case described below indicates the Database Directive can be of influence on the disclosure of geo-databases.

18.3.2 Directive 2003/98/EC on the Reuse of Public Sector Information

Public sector information is data produced and collected by public bodies (digital maps, meteorological, legal, traffic, financial, economic, and other data). A lot of this raw data can be reused or integrated into new products and services which people use on a daily basis, such as car navigation systems, weather forecasts, financial, and insurance services. Reuse of information means that individuals or legal entities can copy, publish, and disseminate the information for commercial and non-commercial purposes. Reuse of this type of information, however, is not a natural thing and needed to be enforced, and therefore, a Directive has been drafted. For outsiders it might speak for itself that information products made by public money should be available to the tax payers for (almost) free, for the governmental institutes producing the information, this seemed not so obvious. Therefore, those institutes needed a push in their backs in order to force them to make available their governmental information.

The Directive on the reuse of public sector information, also known as the Public Sector Information (PSI) Directive, deals with the ways in which public sector bodies should enhance reuse of their information resources. The Directive is built around two key pillars of the internal market: transparency and fair competition. It sets minimum rules for the reuse of PSI throughout the European Union (EU). It also encourages Member States to go beyond these minimum rules and to adopt open-data policies, allowing a broad use of documents held by public sector bodies.

Public sector information has great economic potential. According to a survey conducted by the European Commission in 2006 (MEPSIR 2006), the overall market size for PSI in the EU was estimated at EUR 27 billion.

The main impact of the Directive was intended to be a stimulation of the European information market as a result of improved transparency, the provision

of legal certainty, a framework that encourages a level playing field, the minimizing of competition distortion, conditions that encourage reuse and fair trade, and a downward effect on charges (ePSIplus 2008).

In this Directive, again no special attention has been paid to geo-information. Although in the considerations geographical information is mentioned as a type of information being collected, produced, reproduced, and disseminated by the public sector, and thus of importance in light of the Directive.

18.3.3 Directive 2007/2/EC Establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

This directive lays down the rules for establishing, within the EU, an Infrastructure for Spatial Information (INSPIRE) whose purpose it is to make it possible for interoperable, spatial and environmental data, and services related to these data to be exchanged, shared, accessed, and used. INSPIRE aims to gather users and suppliers of information in such a way that information originating from different sectors will be combined and disseminated.

INSPIRE deals with spatial information such as environmental observations, statistics, etc., that are held in electronic form by or on behalf of public authorities and concern the areas where a Member State has or exercises a jurisdictional right. The information covers themes such as administrative borders, air, soil and water quality observations, biodiversity, land use, transport networks, hydrography, altitude, geology, population and species distribution, habitats, industrial facilities, and natural risk zones.[3]

The Directive wants Member States to make network services available to users so that they will be able to search for, view and download spatial information. These services need to be accessible via an INSPIRE geoportal[4] managed by the Commission at community level, and via additional access points operated by the Member States.[5]

The reasons for initiating INSPIRE were fragmentation of geographical and spatial data, gaps in availability, duplication, data policy restrictions/pricing policies, and the lack of data harmonization. The essence is sharing geographical and spatial data between national public bodies for the purposes of executing public tasks in the field of environment.

It is obvious geo-information plays an important role in this Directive.

---

[3] For a complete list, see Annexes I, II and III of the Directive.

[4] INSPIRE Geoportal, European Commission, http://www.inspire-geoportal.eu

[5] Infrastructure for Spatial Information (INSPIRE), Summaries of EU legislation, europa.eu/legislation_summaries/

18.4 The Directives Evaluated: Is there an Impact on Geo-Information?

Drafting rules is one thing, drafting rules that have an effect, which achieve their goals is another. This is even more complicated in a European Union with so many different countries with different legal histories and traditions. The European Commission is aware of this complexity, and therefore, often evaluates the Directives. Two of the three Directives discussed above—the Database Directive and the PSI Directive—have been evaluated, which gives the opportunity to say something on the impact of the rules, like the impact on the use of databases containing geo-information or the reuse of this type of information, as well as on databases and reuse in general. The INSPIRE Directive had to be implemented by 15 May 2009. On this date far from all Member States had implemented the Directive, let alone already evaluated it. The first reports on the impact of this Directive are expected in May 2010. This means that I can only give general expectations of the impact of this Directive.

18.4.1 Directive 96/9/EC on the Legal Protection of Databases

An evaluation of the Database Directive was published in 2005 by the DG Internal Market and Services. The evaluation pointed out problems associated with the *sui generis* right. The vague terms used in the Directive to define the right had caused considerable legal uncertainty. Also the scope of the right was severely curtailed in a series of judgments rendered by the European Court of Justice (ECJ). The ECJs differentiation between the resources used in the creation of the contents of a database and the obtaining of such data in order to assemble a database demonstrate that the new right has become precariously close to protecting basic information.

The evaluation also mentioned that the economic impact of the Directive on the production of databases is unproved. Looking at EU-based database figures, one could even state the economic impact was none. In 2004, the number of EU-based databases was about the same as in 1998. Strangely enough the European publishing industry considered the *sui generis* protection crucial to the continued success of their activities. Also, respondents to a survey done for this evaluation said to believe that the *sui generis* right has brought about legal certainty, reduced the costs associated with the protection of databases, created more business opportunities, and facilitated the marketing of databases (European Commission 2005).

Despite the reactions of the publishing industry, the evaluators in three options proposed to the European Commission to repeal the whole Database Directive, or to withdraw or change the *sui generis* right being introduced by the Directive. However, they realized that this would have drawbacks as well and would lead to

the resistance of the publishing industry to begin with. Therefore, they also proposed in a fourth option to leave everything as it is. The argument to do so was that, despite its limited effectiveness in creating growth in the production of European databases, the Directive does not impose significant administrative or other regulatory burdens on the database industry or any other industries that depend on having access to data and information. So far, no measures have been taken and no actions seem to be planned to change or repeal the database rules.

No specific data on (the production of) geo-databases were mentioned in the evaluation.

18.4.2 Directive 2003/98/EC on the Reuse of Public Sector Information

The review of the PSI Directive was published on 7 May 2009 (European Commission 2009a). In this review it is stated that the reuse of public sector information is growing. However, far from all the available PSI is being reused. The review mentions several reasons. One of them is already referred to in the introduction of this chapter; the pressure on public sector bodies to finance part of their activities by selling geo-information. The reviewers also write that there is a lack of information on available PSI, and therefore, a fraction of all public sector is being reused.

The situation in the EU seems in contrast with the US, where reuse is strongly encouraged. Citizens and businesses enjoy broad rights to electronically access PSI and have extensive scope for commercial reuse. There is no copyright on federal PSI and there are no restrictions to reuse. Furthermore, fees for reuse are limited to, at most, marginal costs for reproduction and dissemination.

The review makes clear though, that the situation in the EU is improving gradually.

In another study evaluating the impact of the Directive in three main PSI sectors—geographical, meteorological, and legal/administrative—the different indicators monitored to measure PSI reuse highlight market growth and an increase in reuse in all of these sectors in recent years. In the geographical sector, download volumes of PSI in 2007 had grown by approximately 350% since 2002, and in Germany alone the market was estimated to be € 1.5 billion, a 50% increase since 2000 (MICUS 2008).

In this same study, it is concluded that the geographical sector is enriched by new reuser groups which offer innovative applications. As a result the data volume delivered by PSI holders has increased and the income of those holders has grown significantly.

Also it is stated that PSI holders of geographical information are aware of the Directive and that they have introduced a number of changes which are considered to be triggered by the Directive. The PSI holders have carried out improvements which have had effects on the number of products, delivery formats and delivery

speed. Geographical information is also increasingly offered on Internet portals or via web services.

Changes in pricing and licensing have been pursued with less intensity by PSI holders, yet at the same time, reusers complain forcefully about these issues. It is the development of licensing conditions in particular that seems to create difficulties for PSI holders, as the writers of the study pose. Therefore, they state that it is important to improve delivery conditions rapidly. Also because of the fact a recent study by Cambridge University shows that charging nothing or only marginal costs maximizes PSI reuse and that the social and economic benefits far outweigh the immediate financial benefits of cost recovery (Newberry 2008). Marginal cost charging is also one of the key principles of the OECD recommendation for Enhanced Access and More Effective Use of Public Information (OECD 2008).

18.4.3 Directive 2007/2/EC Establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

What the de facto impact of the INSPIRE Directive will be on the disclosure of geographical information is hard to tell, because at the time of writing of this book of 20 Member States, no references on national provisions related to directive 2007/2 were available on the EUR-Lex website. This means most of the Member States have not implemented the directive yet, or at least have not communicated its implementation to the European Commission.

On the other hand, in the report on the reuse of PSI in the geographical, meteorological, and legal information sectors (see note 18), it is has been stated that PSI holders have carried out a substantial amount of improvements for disclosing geographical information. For example, geographical information seems to be disclosed more often on the Internet via portals or web services. The researchers assume that these, more technically driven changes to improve the disclosure of PSI were also promoted by the INSPIRE Directive, which could easily be true since one of the goals of INSPIRE is to establish an infrastructure for spatial information which must be available via access points in the Member States, as well as via a Community geo-portal operated by the Commission.[6] So INSPIRE already seems to have an impact before it has even been implemented in all Member States.

In studies done before the implementation of INSPIRE, several consequences of the Directive have been mentioned (European Commission 2003; VROM

[6] A prototype of the Community Geoportal is already available at http://www.inspire-geoportal.eu

2005). It has been said that within organizations and within the (Dutch) geo-landscape INSPIRE will lead to an acceleration of processes of harmonization, cooperation, and investments.

Standardization and the introduction of geo-portals will lead to an more intensive use and exchange of geo-information throughout the European Union. Also, it is expected that INSPIRE will have an impact on other EU-rules. It could lead to better regulation. If geo-information is wider and easily available, policy makers and legislators will have a better insight which will lead to more consistent (EU) rules at lower costs as well. Of course, INSPIRE will especially benefit the sectors with a strong spatial dimension, including agriculture, regional policy, transport, and spatial planning.

So the impact of the INSPIRE Directive will be found in the easier use and exchange of geographical and spatial data by public bodies in the EU, with all benefits thereof (European Commission 2009b).

18.5 The *Landmark* Case: A Landmark Decision for Geo-Information

The Database Directive and the PSI Directive also played a role in a Dutch case on the reuse of geographical information. Dutch legislation based upon both Directives was discussed in a case which is known as the *Landmark* case.[7]

The case involved Landmark, a private company which had asked the city of Amsterdam for a list of addresses where the city had soil research carried out. The company wanted to reuse these data for its own (commercial) purposes. After a first refusal to provide Landmark with the data, the city of Amsterdam appealed to the fact it had database rights on that particular set of data and that the rules of reuse were applicable giving the city the opportunity to apply conditions to the reuse of the data. The city, therefore, asked for a substantial amount of money before handing over the data, and it also laid down restrictions upon their use.

Landmark disagreed with the city of Amsterdam on the application of these rules and decided to go to court. Before the court, the company stated that the database rules were not applicable because according the rules laid down in Dutch Database Act, the city of Amsterdam could not be considered as the producer of the database. The reasons for drawing this conclusion were that, producing the database containing soil research data did not constitute a risky investment because its production had been funded by public money and, that the data were available within the organization.

[7] In first instance: Rechtbank (Court of first instance) Amsterdam 6 February 2008, LJN BG1554, the appeal: RvS 29 April 2009, LJN BI2651.

The court agreed upon this interpretation of facts and added in accordance with other Dutch case law that database legislation is not applicable to a database which is a by-product of the main activities of an organization.[8] As a result, the article of the Dutch Freedom of Information Act which deals with reuse of public sector information was not applicable either. In the latter case, this was so because those rules are not considered applicable to databases of which a public organ is not the producer. So the Dutch rules based upon the Database Directive and the PSI Directive both were considered not applicable in this case.

The court of appeal reached the same judgment, and also considered the city of Amsterdam not to be the producer of the database containing soil research data.

The fact that the Dutch reuse legislation based on the PSI Directive (also) was not applicable in this case was advantageous for Landmark. That is to say, if those rules were applicable, the city of Amsterdam would have had the opportunity of imposing conditions on the reuse and of asking for a higher price. In this case the city of Amsterdam had no competence to apply conditions to the reuse of the geo-information, as the court in first instance stated. Both courts considered the reuse rules not to be applicable and as a result it was not necessary to give a judgment on the conditions applied by Amsterdam. This was favorable for Landmark, but a pity for impartial observers, because it would have been interesting to know the court's opinion on the conditions applied.

Although the (Dutch) rules in which the Directives are incorporated are not considered applicable by the two courts, they have both decided in the light of the goals of the European Directives. After all, as also being referred to in the case in first instance, public sector information should be widely available and accessible to create opportunities for commercial exploitation of this type of information. The court of appeal referred to the internal market background of the Database Directive to substantiate the point of view that a public body like the city of Amsterdam cannot be seen as a producer of database of addresses. So the impact of Europe on the disclosure of geographical data is obvious in this case. Strange to say, by not applying the Dutch rules in which the Directives are implemented, and yet by judging in line of both Directives.

The *Landmark* case might indicate the direction that the (Dutch) policy of disclosure of public databases of geo-information might go to. After all, as a result of this verdict the chance of a public body producing, managing and disseminating geo-information, and then demanding substantial fees in addition to imposing restrictions on the reuse of such data are rather small. In fact, the decisions were perfectly in line with the objectives of both the internal market and the ideas behind reusing public data. As Marc de Vries of the European Public Sector Information Platform commented, the *Landmark* case was a landmark decision (ePSIplus 2009). Also geo-information professionals consider the case as one with sheer positive consequences. It has been stated in several journals that the

[8] See: Hof (Court of Appeal) Arnhem 4 July 2006, LJN AY0089.

consequences of the *Landmark* case is that no more than the costs of provision of the geo-data can be charged of reuse, and that no excessive restrictions can be imposed (Binnenlands Bestuur 2009).

Concluding, it can be said that the Landmark decision was positive for the disclosure of public sector geo-information in The Netherlands, but the geo disclosure battle is not over. Geo-data is not as easy available as electricity yet, as the chairman of Geo-business Nederland expressed his wishes recently, but a step has been made (VI Matrix 2009).

18.6 Other Initiatives to Improve Dissemination of Geo-Information in The Netherlands

The PSI Directive, and the INSPIRE Directive previously discussed seem to have caused a change in the mindset of policy-makers as far as the disclosure of public sector information is concerned. At least that seems to be the case in The Netherlands. Of course, it is still hard for some public bodies to concede that they have to 'give' away 'their' data to commercial parties, but the chances are high that they are put in place by judges as the *Landmark* case showed. There are also public bodies which take initiatives to disclose public sector information, including geo-information.

The Dutch provinces, for example, have signed a declaration of intent in which they state that they will make geo-information available under as favorable terms as possible. This means information on roads, monuments, flora and fauna will be available to citizens, companies as well as other governmental organizations. This geo-information will be made available the lowest cost possible being the costs of distribution. In addition, restrictions for reuse will be lifted and insight into the quality of the geo-information will be given.

The idea behind this declaration of intent is to give an impulse to the development of innovative products.[9]

A similar initiative has been taken by the district waterboards.[10] They also signed a declaration of intent in which they will make geo-information available at favorable terms. At most, the costs of distribution will be charged and no conditions on use and reuse will be imposed. The district waterboards have information on various sorts of aspects related to the waterways in The Netherlands.

Neither in press releases nor in the declaration of intent is there any reference to earlier documents on public sector information or the PSI Directive. Nevertheless, it speaks for itself that this mindset of public bodies is the result of a campaign for

[9] 'Geo-informatie beter beschikbaar voor iedereen', Dutch Ministry of Interior, 6 December 2007. Search for 'geo-informatie beter beschikbaar' at http://www.minbzk.nl

[10] 'Waterschappen stellen geo-informatie beter beschikbaar', Dutch Ministry of Interior, 24 September 2009. Search for 'geo-informatie beter beschikbaar' at http://www.minbzk.nl

free public information which started more than 10 years ago in The Netherlands and in the rest of Europe (European Commission 1998).

18.7 Conclusion

I have discussed the three Directives in relation to (the disclosure of) geo-information. The Database Directive hardly had any impact in Europe according to the evaluation, at least not economically. It did not lead to a higher production of databases. As far as geo-information is concerned, it is not known whether or not the Database Directive led to a greater availability of geo-information. Since the production of databases in general has not increased, this is probably not the case.

In the evaluation of the PSI Directive it has been said that because of the Directive the reuse of public sector information is increasing. In addition to this evaluation, a study on the PSI Directive showed that the download volumes of public sector (geo) information have substantially increased and the geographical sector has been enriched by new reuser groups which offer innovative applications.

It seems the PSI Directive has urged the public sector to carry out improvements which has had effects on the disclosure of geo-information. For example, in The Netherlands initiatives have been taken by provinces and district waterboards to make geo-information available under favorable terms.

Even before its implementation by all the Member States, the INSPIRE Directive already seems to have had an impact on the disclosure of geographical information. A prototype of the Community geo-portal has been launched by the European Commission and national portals will follow soon. However full implementation of INSPIRE is expected not earlier than 2019 making it hard to predict what the exact consequences of the Directive will be, that more geo-information will be publicly available is without doubt. Whether a greater amount of easily accessible geo-information will result in, for example, more consistent (EU) rules at lower costs, remains to be seen.

In a Dutch lawsuit, the *Landmark* case, in which the Database Directive as well as the PSI Directive played a role, the court judged in favor of a party willing to reuse public geo-information. The judgments referred to the goals of both Directives indicating their influence.

Whatever the future consequences of this case are, the impact of Europe on the disclosure of public sector geo-information is clear and it will be become even clearer when INSPIRE is fully implemented in 2019. Gradually, the goals of the various Directives seem to be achieved. Even the Database Directive, of which it has been said that it hardly had any impact on the database industry in Europe, played a positive role in the disclosure of geo-information at least, in the Dutch decision.

Does this mean that European governments can sit back and relax as far as the disclosure of public sector information in general, and geo-information in particular is concerned? I am afraid not.

Although the result of the lawsuit is positive seen from a PSI perspective, it has been suggested to draft rules clarifying the relation between public sector information and intellectual property rights and to create certainties in respect to the possibilities of (re-)use of this type of information (Eechoud 2008). By doing so, lawsuits like the *Landmark* case could be avoided. In the light of the *Landmark* case and the suggestions made, I am inclined to say that no public bodies should exercise their intellectual property rights on geo-information, if the production of this information is funded by public money and/or if the information is considered to be a by-product of the activities of that public body. Of course, this requires intellectual property management of the public bodies and a property awareness especially when public bodies are cooperating with private parties.

Furthermore, the evaluation and the study on the PSI Directive indicate that pricing and licensing are still an issue and as a result, a lot of potential information is still not being reused (Mulder 2009). There might be growth in the availability of public sector information, but there is no ideal situation so far. In particular it does not appear to be easy to change the policy of public organs which are (partly) financed by the revenues of the sales of geo-information. However, such a change seems necessary to comply with the goals of a European internal market and to achieve the easy accessibility of public sector information.

In this context disputes may arise between PSI holders and reusers on the definition of the public task. Certain public holders' activities are considered added value by the reusers, and therefore, should be produced by the private sector (Fornefeld 2008, p. 40). The public task might need to be redefined as far as the processing of public (geo) information is concerned.

Another aspect often mentioned in this context is related to the quality of the geographical information. What are the consequences for the quality of geo-information, if this type of information is made available at marginal costs? Will a lower price have consequences for the service provided by the public sector, might it even result in the disappearance of certain data sets?[11]

In other words, does a successful European-wide implementation of the PSI Directive have negative consequences for INSPIRE? Can and will European governments guarantee the quality of the geo-data sets made available via the INSPIRE portals? And can they guarantee data sets will not cease to exist?

One could state that European governments are aware of the fact that geographical information is of importance for the national and European markets, thus quality and continuation are assured. However, what will happen in times of crisis?

Put differently, three aspects need further study: the relation of public sector geo-information and intellectual property rights, the definition of the public task related to the adding of value to geo-information, and the guarantee of the quality and continuity of publicly available geo-data sets.

[11] 'Naar optimale beschikbaarheid van overheidsinformatie', Kamerstukken II 1999/00, 26387, nr 7.

References

BDO (1998) Consultants, Elektronische bestanden van het bestuur, under the authority of the Dutch Ministry of Interior

Binnenlands Bestuur (2009) Adressen gratis. 15 May 2009

Eechoud M van (2008) Openbaarheid van bestuur en auteursrecht, never the twain shall meet? In: Eijk NANM van and Hugenholtz PB (red) Dommering-bundel: Opstellen over informatierecht aangeboden aan prof. mr. E.J. Dommering. Amsterdam, Otto Cramwinckel Uitgever, pp 89–100

ePSIplus (2008) Towards the 2008 review of the Directive on PSI reuse http://www.epsiplus.net

ePSIplus (2009) Marc de Vries A landmark decision in the Landmark case! http://www.epsiplus.net

European Commission (1998) Green Paper on public sector information in the information society. COM (1998) 585

European Commission (2003) Contribution to the extended impact assessment of INSPIRE. INSPIRE Framework definition support (FDS) working group, September 2003. inspire.jrc.ec.europa.eu/reports/fds_report_sept2003.pdf

European Commission (2005) First evaluation of Directive 96/9/EC on the legal protection of databases. European Commission, Brussels, 12 December 2005

European Commission (2009a) Reuse of Public Sector Information—Review of Directive 2003/98/EC. COM (2009) 212, Brussels, 7 May 2009

Euopean Commission (2009b) Minutes of the 12th meeting of the Public Sector Information Group. European Commission, Luxembourg, 12 June 2009

Fornefeld Dr M et al (2008) Assessment of the Reuse of Public Sector Information (PSI) in the Geographical information, Meteorological Information and Legal Information Sectors, 2 December 2008

Loenen B van (2005) Implementatie van de EU-Richtlijn hergebruik overheidsinformatie, NJB 6

Loenen B van, Zevenbergen J, Jong J de (2008) Geo-informatie: wat is het en wat is de juridische context? In: Wees L van der and Nouwt S (red) Recht en locatie. Nederlandse Vereniging voor Informatietechnologie en Recht, Elsevier Juridisch, Den Haag

Longley PA et al (2001) Geo-information systems and science. Wiley, Chicester

MEPSIR (2006) Measuring European Public Sector Information Resources. Final Report of Study on Exploitation of public sector information—benchmarking of EU framework conditions. European Commission, June 2006

MICUS (2008) Assessment of the Reuse of Public Sector Information (PSI) in the Geographical Information, Meteorological Information and Legal Information sectors. MICUS, 12/2008

Mulder EJ (2009) Meer halen uit geo-informatie. Automatisering Gids, 18 December 2009

Newberry D et al (2008) Models of Public Sector Information Provision via Trading Funds. Cambridge University, 26 February 2008. http://www.berr.gov.uk/files/file45136.pdf

Nouwt S, Wees L van der (2008) Juridische aspecten van geo-informatie. Commissioned by the 'Alliantie Vitaal Bestuur'

OECD (2008) Recommendation of the OECD Council for enhanced access and more effective use of public sector information, C(2008)38. http://www.oecd.org/dataoecd/0/27/40826024.pdf

Matrix VI (2009) Ed Nijpels 'Geo-data moeten zo makkelijk verkrijgbaar zijn als stroom'. VI Matrix, 128

VROM (2005) Financiële gevolgen INSPIRE-richtlijn. Verslag van een marktconsultatie. Ministerie van VROM, 10 mei 2005

Worboys MF (1995) GIS: a computing perspective. Taylor & Francis, London/Bristol

Zeeuw CJ de, Bregt AK (2007) Vrijgeven van overheids(geo-)informatie. GEO-INFO, 2007-1

Part V
Legal Dimensions: Techno-legal Perspectives

Chapter 19
Sharing Information between Government Agencies: Some Legal Challenges Associated with Semantic Interoperability

Dag Wiese Schartum

Abbreviations

ICT	Information and Communication Technologies
SOA	Service Oriented Architecture
EIF	European Interoperability Framework

Contents

19.1 One Word, a Bundle of Definitions 348
19.2 Local, Regional, and Global Legal Concepts 349
19.3 'Live-in Partner' as an Example 351
19.4 The Problem of Bad Drafting 354
19.5 Fixing Problems Administratively 356
19.6 Court Decisions: Distinguishing the Case 357
19.7 The Problem of Political Control 358
19.8 Conclusion 359
References 361

Contribution received in 2010.

D. W. Schartum (✉)
Norwegian Research Centre for Computers and Law, Oslo University, Oslo, Norway
e-mail: d.w.schartum@jus.uio.no

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*,
Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_19,

19.1 One Word, a Bundle of Definitions

Legislation contains a large number of words and phrases designed to describe legally relevant aspects of citizens' lives. A large volume of legislation is linked to various governmental schemes. 'Income', 'married', 'number of children you support' are examples of words and phrases describing data collected to serve as the basis for individual administrative decisions. Identical wordings are often used in several pieces of legislation, a practice that may create the expectation that relevant collected data could be shared between government bodies. For example, it might be expected that expressions such as 'residential address' have identical semantic content throughout national and even European legislation, thus making it possible to design information systems with shared information across regulatory and administrative borders.

The sharing of 'basic data' across organizational borders in government administration has been an important objective in the Norwegian public sector's modernization process for at least 40 years. This focus has resulted in the establishment of several information systems with the clear aim to serve broad areas of government administration. The Population Register, The Central Coordinating Register for Legal Entities, The Register of Reporting Obligations of Enterprises and The Employer/Employee Register are examples of central government information services in Norway designed to provide services across sectors, agencies, and administrative levels.

Current Norwegian efforts to increase the sharing of information between government agencies are in line with European Interoperability Strategy.[1] The Norwegian Ministry of Government Administration and Reform is currently evaluating the overall ICT architecture, using a Service Oriented Architecture (SOA) approach.[2] Emphasis is partly on improving the availability of general registers, and partly on developing overviews of metadata and data definitions, preparing the ground for increased use of data across government borders.[3] Most of these initiatives are implemented using an information systems approach, and the fact that a large fraction of data definitions have their origins in legal sources is not emphasized.

The first European Interoperability Framework (EIF) was published in 2004, representing a rather simple approach focusing on the ability of ICT systems to support exchange of data and thereby share information and knowledge. EIF version 2.0 (2008) and later documents represent a considerably broader view of interoperability as EIF encompasses six layers that must be addressed individually: political context, organizational interoperability, legal interoperability, semantic

[1] See European Commission 2009.

[2] See the report Ministry of Government Administration and Reform 2007.

[3] One important effort is the development of a central semantic register for electronic cooperation (Semantikkregisteret for elektronisk samhandling—SERES), see http://www.brreg.no/samordning/semantikk/index.html

interoperability, and technical interoperability.[4] In this chapter I will discuss selected issues in the legal layer regarding first and foremost the nature of legal definitions. This chapter will explore possibilities and obstacles associated with semantic interoperability in the legal domain, using examples from Norwegian legislation.

19.2 Local, Regional, and Global Legal Concepts

As a simple point of departure, words may be described as having a vague or fixed meaning.[5] It is probably fruitful to think of vagueness as the dominating aspect, in the sense that vagueness and uncertainty concerning how words should be understood is the core problem. Thus the degree of vagueness decreases on a scale running from 'very vague' at the one end and 'rather fixed' at the other end. Even words we might perceive as maximally fixed may be encumbered with uncertainty. Although 'man' and 'woman', for example, are words with a very fixed interpretation, transsexuals may nonetheless challenge this otherwise clear semantic content.

Here, I wish to make a distinction between fixed words outside and inside the legal system, i.e., words that are fixed and independent of the legal system, and words that are fixed by the legal system. The first group is represented primarily by words linked to rules/conventions within the fields of mathematics and the natural sciences. Examples are words denoting measurement (kilo, meter, hour, etc.) and words used within scientific systems to describe natural things and properties (flowers, mammals, gender, diagnoses, chemicals, etc.). The common denominator for these words is that they are defined within a scientific system which is generally accepted. They are thus 'global' in one sense. Such scientific words have fixed interpretations independent of law, and are often used within laws according to accepted linguistic norms. The legislator will hardly define 'dog', 'DNA', 'hour', etc., and if defined, it would be exceptional if something other than a scientific definition were to be used.[6] Information linked to this group of words with a fixed meaning may easily be shared between many organizations and may thus be part of a semantic infrastructure in government administration and elsewhere. However, to formulate legal rules within various aspects of society, we obviously need many more words/expressions than those offered by science.

---

[4] EIS 2.0 states that interoperability can be affected by 'differences in legislation in areas such as administrative law, identification and authentication, intellectual property rights, liability, privacy and data protection, public administration transparency relationships between public administrations, citizens, businesses and other IT actors and the re-use of public sector information in base registries' (p. 34). Cf., European Commission 2009, Section 4.2.1.4.

[5] Cf., Bing 1986.

[6] Contrasting scientific definitions may exist (for instance for the term 'biometrics') which create a need for the legislator to make a choice.

Words and phrases are the building blocks of legal provisions, often as elements of legal conditions and results. Vagueness in natural languages often makes it possible to understand a word or phrase in several different ways, in specific contexts. Vague words may thus make legal provisions hard to interpret and apply, in turn creating the need to make words in legal provisions more fixed.[7] In this respect, I will introduce four ways of making concepts within the legal system more fixed.[8] A common characteristic is that all methods represent legal decisions regarding what the meaning of a word/expression should be (definitions).

In the Norwegian style of legislation, definitions are not necessarily contained in the statutory text itself, but are introduced in the preamble of the act, in particular in the statements giving grounds for and explanations of the various provisions. This practice is rather common. Such definitions are often in-exhaustive but center on what the legislator perceives as the particular issue and/or important elements in the course of interpretation.

A second type of definition is the introduction of rules containing scattered definitional statements, i.e., statements that clarify certain potential ambiguities regarding the meaning of specific legal words. One of many examples in Norwegian legislation is found in the Health Personnel Act, Section 66, where it is emphasized that

> The word employer also includes any public authority that the relevant health personnel have entered into an agreement with relating to the running of a practice.

Such definitional elements are usually strictly local; i.e., they will have an impact only within the scope of the legislation in question.

Legal decisions regarding the meaning of words and phrases often occur as explicit statutory definitions, typically listed in the introduction of a piece of legislation. Usually such definitions are only local, i.e., they are only valid and binding within the framework of the body of rules in question. The scope of certain definitions may, however, be broadened through new decisions, either in provisions repeating definitions in other legislation or by clearly stating that these definitions shall apply. The latter technique, for example, is employed in the Data Retention Directive Article 2 (1)[9] which stipulates that all definitions of three other directives shall apply.[10] I designate definitions with a scope covering several but a limited number of statutes as 'regional definitions'.

---

[7] The term 'more fixed words', however, does not necessarily imply simpler and less complex definitions, but merely that words are defined in ways which make them easier to interpret and apply.

[8] This of course does not claim to be an exhaustive specification.

[9] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[10] The cited directives are Directive 95/46/EC, Directive 2002/21/EC and Directive 2002/58/EC.

The techniques referred to above that explicitly state local and regional definitions are very different from the fourth approach in which legislation (e.g., an act or part of an act) is passed entailing that global *de facto* definitions are established. In other words, these are definitions from which there can hardly be any deviation within the legal system, unless a definitional variant is explicitly laid down. In Norway, for instance, it is not feasible to use words such as (in translation from the Norwegian) 'marriage,' 'limited company', and 'citizenship' in rules of law without, respectively, relating to the Marriage Act, the Limited Liability Companies Act, and the Norwegian Nationality Act. This effect is not necessarily due to the fact that these laws clearly state their general authoritative significance, but can just as often be explained by their role as *de facto* predominant legal sources for the interpretation of the mentioned words. 'Live-in partner', by comparison, is not defined or regulated in a similarly authoritative way, which in turn allows ample leeway for legislators who wish to define and contextualize this word.

Common to these four types of definitions within a Norwegian legislative style is that techniques 2–4 are combined with technique 1. Definitions, in other words, may be found both in the statutory text itself and in the preamble of the act, in particular in the grounds/explanations of the laws.

In the following discussion, focus is on identifying arguments in favor of definitions that may be shared between several government agencies, and in particular possible limitations in a development toward semantic interoperability. The discussion will illustrate important relations between policy-making, law, and the development of information systems.

19.3 'Live-in Partner' as an Example

The Norwegian word 'samboer' (English: literally 'live-in partner') denotes a close, spouse-like personal relationship, cf., 'common-law spouse' and 'cohabitant.'[11] In a linguistic sense, however, the term 'live-in partner' is quite ambiguous and opens for the argument that it may also denote people of the same sex living together outside a sexual relationship (e.g., friends, brothers, and sisters). The common expectation, however, would be that 'live-in partner' denotes people living together as if they were married. Not withstanding this, outside a particular context the definition of the word is generally uncertain and occurrences of the word in legislation may require thorough interpretation in order to establish a correct definition. Different definitions obviously entail problems when sharing data between relevant government agencies, whereas identical definitions may open for more cost-effective information management, where one branch of

[11] 'Cohabitant' is often used as the English translation for 'samboer' in Norwegian legislation. I have chosen to use 'live-in partner' instead, because I see this translation as most open to interpretation in terms of the three possible English concepts.

government may supply several or all other parts of government with information concerning this social group.

A search in Norwegian legislation reveals that the expression 'live-in partner' occurs in 36 different Norwegian Acts of Parliament. The word is also used and defined in a large number of regulations, i.e., provisions pursuant to delegated legislative power. In this article I will limit the discussion to four central examples of legislation where 'live-in partner' plays an important role.[12] I use these occurrences to identify and discuss some of the legal problems associated with sharing this type of information across legal and institutional borders.

I will not go into detail here regarding the four parliamentary acts constituting the bases for the following exemplifications but will instead restrict explanations to my categorization of the various conditions embedded in the various definitions[13] of 'live-in partner' as stated in the four Acts. I have numbered each act 1–4. The table below shows the types of definitional conditions that are used in each of the acts in question. In all, fourteen different conditions are identified, whereof all but two are used in only one of the analyzed acts. However, although most conditions are unique within the selection, clear similarities and close relations exist between several of them. Such close relations are made evident by means of five categories of conditions provided here by the author (Table 19.1).

The table is the result only of analyses of statutory texts and preparatory documents from the legislative process. It does not mirror interpretations and practices from case law, and thus presents a simplified picture.

Only one act clearly states that live-in partners must be at least 18 years old, but conditions regarding marriage, etc. imply age limits, because people younger than 18 years of age are not allowed to marry without a special permit.[14] Three of four acts establish conditions regarding accommodation. In the fourth act this condition is embedded in a discretionary condition regarding stable and established relationship between the partners, a provision which normally implies joint accommodation. Accommodation is both linked up to the formal condition of having a joint address and to factual descriptions of how accommodations are used. In one of the acts, it is required that partners live in the same accommodation, while the provisions of another act permit them to live in different accommodations within the same household, unless there are four or less separate accommodations in that house(!). Two of the acts accept that partners may temporarily live apart, but one of these excludes cases in which separation is caused by imprisonment of one or both of the partners. The two acts which require certain duration of the relationship

[12] The following Acts comprise part of my investigation: Act concerning the entry of foreign nationals into the Kingdom of Norway and their presence in the realm, Act on Norwegian nationality, The National Insurance Act, and Act concerning individual pension agreements.

[13] Use of the word 'Definitions' here does not imply that a formal definition is explicitly formulated. Definition is rather the result of my interpretation of the term 'live-in partner,' as it is understood in the statutory text and preparatory works of the acts.

[14] With 16 years as absolute minimum age for marriage.

Table 19.1

Category	Conditions	Act no.
Personal	More than 18 years old	1
Accommodation	Joint address	2
	Joint accommodation	4
	Living in the same house with less than four separate accommodations	3
	Temporarily apart	3
	Temporarily apart excluding imprisonment	2
Life together	Stable and established relationship as live-in partners	1
	Intention of continuing to live together	1
	Joint housekeeping	2
Duration	Of live-in partnership	1
	Of relationship similar to marriage or registered homosexual partnership	4
Children	Are parents to joint children	1, 3, 4
	Have been parents to joint children	3
Marriage, etc.	Have previously been married	3
	Marriage would have been legal	1, 2, 3, 4
	Registered homosexual partnership would have been legal	2, 4

between people wanting to be accepted as live-in partners describe this relationship differently, and the conditions are thus unequal.

Three of four acts require that the partners have joint children, while one of them also recognizes the eventuality that they have been parents, i.e., that the children are deceased. The last type of condition in the table refers to marriage and registered homosexual partnership.[15] One of the acts accepts a couple as live-in partners if they have been married previously, even though they are without children. All four acts require (directly or indirectly) that marriage would have been legal between those wishing to be accepted as live-in partners, a condition that should be read with reference to additional eight conditions for entering into marriage pursuant to the Marriage Act.[16]

This superficial examination of various elements embedded in the definition of the term 'live-in partner' obviously provides an incomplete picture of each set of legal regulations regarding such partnerships. On the other hand, it provides us with a useful example of the possible complexity behind an apparently simple word. In the conclusion of this chapter I will illustrate how 'live-in partner' may be defined in order to serve as a common, basic definition in several acts.

[15] Such partnerships were previously registered pursuant to Act relating to registered partnership, but a unified Marriage Act was approved in July 2008.

[16] Cf., Act of 7th April 1991 No. 2, Sections 1–5a.

19.4 The Problem of Bad Drafting

Lawmaking reminds us of the close relationship between politics and law, in the sense that to a large degree law express politicians' opinions. Lawyers are in the service of both the political and the legal system. In the first phase of lawmaking, politicians often formulate a mandate containing guidelines for legal experts and others sharing the task of drafting legislation. Many countries have technical norms regarding how laws should be drafted, e.g., how provisions should be numbered, how references to other legislation should be made, etc. In Norway for instance, the Ministry of Justice and the Police publish guidelines concerning regulatory technique as the basis for regulatory control by the Ministry of most new laws.[17] However, these guidelines first and foremost address technical and formal questions (layout, reference techniques, etc.) and thus represent a rather limited approach to lawmaking. No fixed method is applied for the development of statutory texts and most laws, to a large extent, are drafted free-hand.

One important effect of 'legislation ad lib' is that there is no standard expectation regarding investigation and analysis of words embedded in draft legislation. For instance, if a regulation requires a word designating spouse-like relationships, they are likely to choose 'live-in partner' and introduce the sets of conditions and definition they find suitable, without investigating whether one of the already existing definitions of the word in other parts of legislation will suffice. I have not conducted thorough surveys of the preparatory works of the four acts analyzed in Sect. 19.3 (above). Publicly available preparatory works indicate, however, that investigation into occurrences of 'live-in partner' in other legislation was carried out only in conjunction with one of these acts. No other references to existing definitions are made, at least, in the explanatory texts, etc. However, a closer look at the differences between the four sets of regulations gives rise to the suspicion that several of these differences would not survive attempts to compare and harmonize them with one another. To illustrate this point, let us go back to one of the main categories of conditions defining 'live-in partner' in the four sets of legal regulations (Table 19.2).

My first comment relates to the fact that Act 1 does not address the question of accommodation at all, but rather places this issue within an evaluation of whether a stable and established relationship between live-in partners exists or does not exist. Thus it is very unlikely that the introduction of a condition regarding accommodation would create any problem. My second point concerns the choice between 'joint address,' 'joint accommodation', and 'same house with less than four separate accommodations.' 'Same house…' seems to be more liberal than 'joint address' and 'joint accommodation,' but it cannot be excluded that all three alternatives may express the same meaning. The choice of 'joint address' instead of 'joint accommodation' may be motivated by the fact that the first alternative

[17] Ministry of Justice and the Police Ministry of Justice, the Police 2000.

Table 19.2

Category	Conditions	Act no.
Accommodation	Joint address	2
	Joint accommodation	4
	Same house with less than four separate accommodations	3
	Temporary apart	3
	Temporary apart if not imprisonment	2

indicates an officially registered residential address (i.e., a formal criterion), while 'joint accommodation' may be interpreted as denoting how couples actually live together. Notwithstanding this, in my view it would probably be feasible to establish one common criterion describing accommodation/address. A third point is that only two of four acts address the irregular situation involving partners who are temporarily living apart from one another, and not sharing accommodation. This situation may occur in any live-in partnership relationship and must thus always find a legal solution. Imperfect regulation of such occurrences may thus be seen as an example of faulty legislation and insufficient definition of 'live-in partner'.

My 'speculative' discussion of possible explanations for differences seeks to make probable that in the case of 'live-in partners' there are unexploited possibilities to establish common criteria and definitions. From the viewpoint of lawmaking, the question is if it is feasible or not to offer policymakers certain standardized words to describe political objectives. From a policymaking perspective on the other hand, the question is if such definitions are adequate for the expression of political objectives.

Lawmaking is one of the very few government decision-making processes in Norway (and I believe in many other countries) that is largely performed without ICT tools especially developed to support that type of decision (Schartum 2008, pp. 17–33). Here, I will not go into general questions concerning such tools, but will merely underscore that tools supporting text retrieval and analysis of legal words that could be shared and jointly employed in several pieces of legislation are desirable. Appropriate tools will make it relatively easy to compile a corpus of synonyms occurring in other relevant legislation.[18] Existence of such tools does not necessarily imply that only existing definitions should be used in the drafting of new laws. Even when the legislator chooses to author additional definitions, knowledge and cross-referencing with existing legal definitions, for example, may yield a more thorough preparatory consideration because one can learn from existing definitions even though these are not used. The legislator may, for example, become aware of the need to consider the issue of whether people should be accepted as 'live-in partners' even though they temporarily have separate accommodations because of imprisonment and other events, cf., the above.

[18] Other possibilities are sketched in Schartum 2008, pp. 35–66.

Introduction of global and regional concepts across legislation and information systems is in my view realistic only if computerized tools are developed to help lawmakers identify and analyze relevant words and concepts. Unless such tools are introduced, the chances are high that legislation will be produced which, for no valid political reason, carries provisions containing awkward use of words/concepts that in turn create problems to be solved in the appurtenant information system, cf., next section.

19.5 Fixing Problems Administratively

Bad drafting could be compensated by means of 'creative solutions,' based on the view that different definitions are sufficiently similar to be handled in a shared computerized routine. In other words, even if the legislator fails to harmonize data definitions and make it difficult to use data from external sources, it is possible, on the information system level, to partly compensate for this shortcoming. The condition is that differences between data definitions are not too great. Definitions of live-in partner in two sets of regulations, for instance, may be almost identical, aside from certain elements which are expected to be of significance in a small percentage of cases. If so, the strategy could be to share information on the basis of one of two procedures.

i. A special routine is established to handle cases where definitional differences have an impact.
ii. Alternatively such differences are disregarded as a part of the initial, ordinary administrative decision-making process. Instead, definitional differences are handled in the course of processing complaint cases.

An information system may, for instance, be based on the assumption that 90% of those accepted as live-in partners pursuant to regulation A should be accepted as live-in partners pursuant to regulation B. The handling of these B-cases may thus be based on the results in A-cases, for example by means of a computerized routine. The assumed 10% of the cases where the computerized routine alone would give incorrect results may be intercepted by manual routines. Knowledge of the differences between definitions for 'live-in partner' in regulation A and B, make it possible to specify assumed, uncertain elements on which individual decisions are based. Parties may be asked to check this assumptions/information and give notice or make a complaint to the authority. Decisions in B-cases are based on the assumption that people having the same residential address (as established in A-cases) share accommodation (as required in B-cases). Negative decisions in cases where people share accommodation without having registered a joint address may then be subject to complaint. In positive decisions where people have a joint address but do not physically share the accommodation, parties to the case may be obligated to notify the authority so the decision may be corrected. A radical alternative would be to drop manual routines to correct bases of

decisions and instead assume that the number of errors originating from differences between definition A and definition B is acceptable, given the right for parties in individual cases to make a complaint.

There are of course several objections that could be made to the suggested administrative solutions. Use of almost identical types of information in individual cases implies use of a certain amount of incorrect data as a basis for decisions. Obviously, the quality requirement should, at least as a point of departure, be 100% correctness. Moreover, to rely on people to lodge complaints or give notification in order to correct errors is obviously to gamble with quality requirements. However, the promise of cost reductions associated with the use of information from shared machine-readable sources, which in turn makes the collection of information from each individual party redundant, is an attractive benefit to be gained.

19.6 Court Decisions: Distinguishing the Case

Citizens in a society under rule of law may bring their cases before the courts and independent appeal boards to test the correctness of administrative decisions. A person denied 'live-in partner' status may for instance petition the court to render another decision. To a certain extent the courts mirror societal change, etc., meaning that definitions of concepts may not be 100% stable but rather dynamic and reflect societal change without formal amendment to statutory law. For example, people who were not accepted as live-in partners 5 years ago may be granted this status today due to new circumstances which the legislator had not considered.

An example from the National Insurance Court serves to illustrate the point.[19] The granting of pension benefits was conditioned by termination of A and B's live-in partnership. The court concluded that although A and B still lived together every now and then, they could no longer be considered live-in partners. The main reason was that B had acquired his own accommodation. The court introduced a new explicit element relevant to the interpretation of 'living in the same house' by qualifying ownership of two accommodations as a decisive factor.

In other words, court decisions may establish new elements in the definition of concepts in addition to those embedded in legislation with explanatory comments in preparatory works of the act. This dynamic nature of law is obviously challenging for development and maintenance of information systems designed to create semantic interoperability between government agencies. One of the implications is that even though the legislator at one point in time may manage to coordinate various fields of law and formulate a joint definition shared via a

[19] Cf., case TRR-2003-04771.

common information system, court decisions may at any given point in time imply a change of definition and thus endanger this harmony. Court decisions will usually not have an impact on related fields of law. Thus it will usually not be possible to allow such decisions to affect other fields of law sharing the same definition of concept in a joint information system.[20] Court decisions, in other words, may create an unavoidable problem in attempts to establish shared information.

The court's power to distinguish the case, i.e., to make concrete judgments in cases and eventually identify new elements in the interpretation of law is important in order to safeguard fairness for the individual in the legal system. An ideal solution seen in the perspective of information systems would be to pass legislation explicitly stating that definitions of concepts shall be identical with corresponding definitions in certain other parts of legislation (cf., *supra*, Sect. 19.2, the example on legal decisions regarding the meaning of words and phrases). In this way courts may be obliged to consider definitions for all relevant laws jointly. Other solutions may be to change the information system in accordance with changing case law or to establish compensatory manual routines.

19.7 The Problem of Political Control

Political views and processes are dynamic and legal regulations are amended accordingly. Amendments, for example, may be triggered by mass media headlines that result in pressure on politicians. Such situations may be occasioned by incidents which people find clearly unfair and for which they demand political change. Unfairness and appeals for political, and subsequently legal, change may impact on concepts in the wording of provisions such as, in the foregoing example, the term 'live-in partner.' Even though the legislator has been able to draft laws with jointly defined words, a demand for amendment will easily destroy this apparent harmony. What may begin as common definitions may be fragmented by subsequent political developments. In this event, information sharing will be made difficult or impossible.

When legislators choose the formulation of legal rules, they partly make a prediction regarding which wording will be most suitable to realize the political objectives pursued through that law. Predictions of course always entail a degree of uncertainty. Uncertainty is easier to avoid if an appropriate degree of ambiguity and discretion is embedded in the provisions from the outset. An important prerequisite is that interpretations are made in line with provisions expressing the aim of the act, entailing that vague expressions, etc., are understood pursuant to the assumed will of the legislator. Such linguistic qualities and regulatory techniques yield a certain degree of flexibility in the application of the law and consequently a

[20] Unless, of course, the act is amended.

better opportunity to tackle situations that the legislator did not consider when the law was passed.

From a political viewpoint, deliberately vague definitions in statutory texts are not necessarily negative. The careful inclusion of vagueness, on the contrary, may pave the way for information systems that are as efficient as possible in a legal context. On the other hand, one may certainly not conclude that the vaguer a legal text is, the better political control will be. The challenge, as is often the case, is to strike the right balance. In the next and concluding section of this article, I will investigate this balance further.

19.8 Conclusion

An important underlying issue in this article has been the tension between the rather flexible, open and discretionary legal system, and the rather formalized, closed and inflexible computerized information systems. Discussions have demonstrated that it is difficult to go far in the direction of formalizing words and phrases used in legislation without clashing with important legal principles. Thus, solutions are probably to be found between the extremes by choosing a middle course in which both legal principles and effective administration and information systems could be accommodated.

In Sect. 19.2 above, I identified two major techniques that may be implemented in order to establish regional or global definitions of words and phrases describing data that we claim public administration and other institutions can share between them. One of these concerned statutory definitions (cf., Sect. 19.3) and another referred to legislation with general impact (cf., Sect. 19.4). In concluding, I will develop the latter strategy in order to illustrate how vagueness and formalization could be combined and still allow more information to be shared.

Government administration usually has a monopoly on the exercise of power within its field of specialization: Only one agency has the power to levy income tax, assign various types of benefits according to compulsory arrangements (sickness, unemployment, retirement, etc.), approve the establishment of companies, approve marriage and divorce, sentence criminals, issue certificates for firearms and driver's licenses, approve motor vehicles, etc. These types of government monopolies imply that there can be only one primary source of information regarding such decisions, and by extension that when decisions are final (with no further right of lodge a complaint), the information is regarded as true and stable. Such information is much easier to share between government agencies and other organizations than other types of information. Limitations on the widespread use of such government information is first and foremost linked to considerations regarding data protection and privacy and related in particular to the purpose specification principle in European data protection law (Bygrave 2002, p. 61). Such considerations will not be discussed here, however.

In this context, I will also submit the possibility of using information from individual decisions in government agencies as building elements in the construction of new concepts. For example, we may define a basic concept for 'live-in partner' only on information that has been established as legal fact and been registered in government files.

P1 and P2 are live-in partners if
P1 and P2 have identical residential address in the Population Register
P1 and P2 are not registered as members of the same family in the Population Register
P1 and P2 are not registered as a married couple in the Marriage Register

As emphasized in the discussion of political control, it is often undesirable to limit legislation to a few highly formalized facts and criteria as exemplified above. Such formalization could, however, be a prefabricated element and serve as the basis for further political consideration. Other conditions could then be suggested, beyond this basis, as options for policymakers. In the case of defining 'live-in partner' in more subtle terms than those seen in the statements above, additional elements might be:

P1 and P2 are live-in partners if
(basic fixed conditions, cf., above) and if
P1 and P2 live in the same house with less than four separate accommodations according to the Population Register
P1 and P2 are older than 18 years of age according to the Population Register
P1 and P2 temporarily live apart according to the Population Register

In this second layer of definitions, policymakers may have a choice of additional elements to consider as conditions for qualification as a live-in partner. The exemplification (above) uses fixed conditions, i.e., conditions that refer to information established in government files according to authoritative decisions and other registrations of facts. A second/middle layer of this type may be skipped and/or be replaced/supplemented with a third layer of possible and optional conditions which lawmakers may consider. On this level, conditions require concrete evaluation in each individual case, and contain vague, rather than discretionary, elements. The following examples are based on actual definitions presented in Sect. 19.3 (above).

P1 and P2 are live-in partners if
(basic fixed conditions, cf., above) and if
(optional fixed conditions)
P1 and P2 live in a stable and established relationship
P1 and P2 have the intention of continuing to live together
P1 and P2 have joint housekeeping

The idea is not to restrict lawmakers' possibilities in formulating fair legislation by laying down fixed and 'square' definitions, but instead to introduce a framework to which special elements may be added on the basis of political considerations.

The basic definition of 'live-in partner' (above), for example, may not be appropriate or applicable within all types of legislation, and in this event, supplementary information concerning fixed and/or vague conditions may be considered. However, possibilities of automated supply of relevant and relatively inexpensively obtained information associated with the first two layers of definition will—very likely—increase the chances that lawmakers will avail themselves of these and be reluctant to use comparatively more expensive information regarding vague criteria on the third level.

This very tentative sketch for how words/concepts may be constructed on the basis of decisions or other conclusions reached in government administration may be attributed to the kind of aspiration traditionally labeled 'computer-friendly legislation'. In other words, attempts such as these may be ascribed to the need to adopt legislation which could be, more easily than today, transformed and implemented in computerized information systems. The label 'computer-friendly legislation', however, may very well conceal basic problems in terms of legislative management and application. 'Computer-friendly' may be largely synonymous with 'well-defined,' and well-defined legislation is a paramount prerequisite for comprehensible legislation. Clearer definitions of legal concepts and economy of numbers of definitions are therefore not only a benefit for public administrators in their effort to achieve more efficient government through information sharing between government agencies; consolidation and harmonization might be seen as equally valuable for ordinary citizens trying to make their way through the jungle of legal rules.

References

Bing J (1986) Om tolking av enkeltord—særlig I lovtekst [On interpretation of single words in texts of Acts]. In: Bratholm A, Opsahl T, Aarbakke M (eds) Samfunn, rett, rettferdighet. TANO A/S, Oslo

Bygrave LA (2002) Data protection law. Approaching its rationale, logic and limits. Kluwer Law International, The Hague

European Commission (2009) Directorate General for Informatics, Supporting the European Interoperability Strategy Elaboration, Final Report Phase 1, Deloitte 2009. http://ec.europa.eu/idabc/servlets/Doc?id=32207

Ministry of Government, Administration Reform (2007) Felles IKT-arkitektur i offentlig sektor (Joint ICT-architecture in Public Administration). Ministry of Government Administration and Reform, Oslo

Ministry of Justice, the Police (2000) Lovteknikk og lovforberedelse [Regulatory Technique and Preparation]. Ministry of Justice and the Police, Oslo

Schartum DW (2008) It-støtte for arbeid med lovsaker (Support of legislative processes by information technology). Complex 4/2008, Unipub

Chapter 20
Public Information Infrastructures and Identity Fraud

Jan Grijpink

Contents

20.1 Introduction 364
20.2 Chains and Chain Cooperation 364
20.2.1 Chain Issues 364
20.2.2 Concepts of 'Chain', 'Dominant Chain Problem' and 'Chain Level' 365
20.2.3 Chain Thinking 366
20.2.4 The Scientific Relevance of the Chain Concept: Fallacy of the Wrong Level 366
20.2.5 Example: The European Union's Biometric Visa System 366
20.2.6 Remedies Offered by the Doctrine of Chain Computerization 368
20.2.7 Chain Research Results in the Chain Dimension 369
20.3 Identity Fraud (Identity Theft) 370
20.3.1 The Concept of Identity Fraud (Identity Theft) 370
20.3.2 Identity Fraud, a Growing Problem 371
20.3.3 Chain Research Results in the Identity Fraud Dimension 373
20.4 Identity Fraud in the Criminal Law Enforcement Chain 373

Contribution received in 2010.

A brief introduction was published in two articles in Information Infrastructures and Policy 6 (1997–1999), IOS Press, Amsterdam, March 2000: (1) Chain computerization for inter-organizational policy implementation and: (2) Chain computerization for better privacy protection.

J. Grijpink (✉)
Emeritus professor of information science
Utrecht University, Utrecht, The Netherlands
and
Former information strategist
Dutch Ministry of Justice
The Hague, The Netherlands
e-mail: jan-grijpink@ziggo.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_20,

20.4.1 Identity Fraud in the Dutch Criminal Law Enforcement Chain 373
20.4.2 Identity Fraud in the Criminal Law Enforcement Chain at EU Level..... 376
20.5 Some Conclusions and Challenges 379
20.5.1 Conclusions 379
20.5.2 Challenges 379
References 380

20.1 Introduction

During the past 4 years, more than twenty Dutch large-scale chain cooperation cases have been studied in the chain research program at the Institute of Information and Computer Sciences of Utrecht University, using the guidelines and the chain analysis tools provided by the doctrine of chain-computerization. This chain research program has led to some valuable insights and breaking views with regard to both public information-infrastructures and identity fraud. The chain perspective focuses on the interplay of forces that determine the effectiveness of large-scale information exchange; the perspective of identity fraud focuses on the fact that the misuse of somebody else's identity leaves behind many traces that, however, point towards the victim instead of towards the culprit.

First, the chain perspective and the identity fraud perspective are introduced and some interesting chain research results mentioned. Then, we combine both perspectives to understand the case of identity fraud in the Dutch criminal law enforcement chain and its international extension involving the EU exchange of criminal verdicts. Finally, we draw conclusions and highlight major challenges.

20.2 Chains and Chain Cooperation

First of all, the chain perspective is introduced. Large-scale chain information-infrastructures provide a better understanding of the menacing prospects of identity fraud with regard to our privacy and security.

20.2.1 Chain Issues

Barely a day goes by without chain issues making the news. Today's headlines are about terrorists' attacks and football hooliganism, tomorrow's about juvenile delinquency and medical errors due to faulty data transfer. We are thus confronted with many large-scale chain issues that are difficult to resolve. These issues always involve the large-scale exchange of information among huge numbers of more or less autonomous organizations and professionals. No single chain partner has the power to compel other chain partners to cooperate effectively. Moreover, they are often confronted with sloppy compliance or sometimes even with direct hostility or opposition by the persons involved: e.g., a forgetful patient, an angry citizen or a

suspect. If something goes systematically wrong with the communication in a chain, many wrong decisions are made, that the chain becomes disrupted and discredited.

20.2.2 Concepts of 'Chain', 'Dominant Chain Problem' and 'Chain Level'

'Chain' does not mean logistics (the process of handling goods) that we so often come across in the business community, nor an information chain (closely linked information systems) nor a chain of transactions (subsequent transactions within a process). The chain concept is used here explicitly to refer to social chains such as social security, criminal law enforcement or drug addict's health care: large-scale inter-organizational processes that yield a social product such as income support, safety or survival (See Fig. 20.1).

In a social chain, thousands of organizations and professionals work together without a clear relationship of authority, in ever-changing combinations depending upon the actual case. However, cooperating with other organizations and professionals takes a great deal of effort, time and money. There must be a cast-iron reason for doing so. One important element of the chain concept introduced here is, therefore, that chain partners only cooperate if they are forced to do so by a dominant chain problem. A dominant chain problem is one that none of the partners can solve on its own. It is only by effectively cooperating that chain partners can prevent the systematic failure of their own organization and the entire chain.

Such a barely-manageable problem creates an interplay of forces which triggers large-scale cooperation of so many organizations and individuals, and promotes the development and maintenance of a large-scale chain communication system. However, in most chain cooperation situations, this condition is not yet fulfilled. The identity chain, for example, cannot prevent your identity from being misused—undetected—by someone else. If only one organization inadvertently

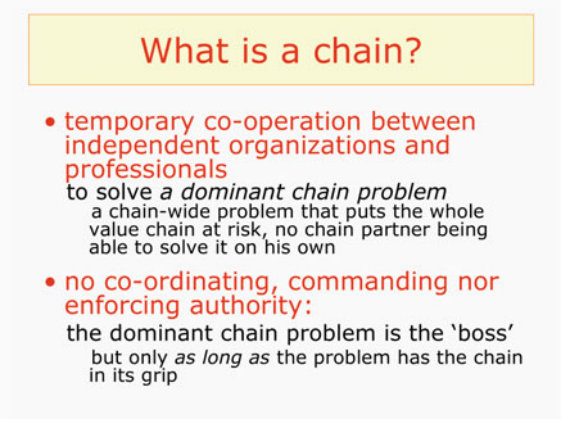

Fig. 20.1 The chain concept

accepts a deliberately mistaken identity, the identity fraudster can use it anywhere else without arousing suspicion.

20.2.3 Chain Thinking

Chain thinking is gaining importance. Advancing specialization and mounting social requirements make private and public organizations and professionals increasingly more dependent on each other. However, chain cooperation proves to be anything but easy, in practice. Because common interests are less pronounced than people usually think—and are also often unclear—the badly needed cohesion can only be provided by a pressing dominant chain problem. Only then is there sufficient support for the large-scale exchange of information.

As overall leadership or authority is absent, the chain is a difficult administrative domain in which decision-making and information exchange proceed differently, than within organizations. Rationality and efficiency are often hard to find at the collective chain level and as a consequence, unpredictability and lack of control are the order of the day. Put simply, chains form a bleak working environment. However, that is nonetheless where the computerization of society is—to a significant extent—taking place, thus determining the quality of life in the future information society.

20.2.4 The Scientific Relevance of the Chain Concept: Fallacy of the Wrong Level

Information science derives its core concepts and theories from several disciplines and sub-disciplines. We are familiar with the idea that knowledge is only valid within the boundaries of the theoretical framework from which it has been gained. Combining concepts from different theoretical frameworks is a permanent challenge. Even when applying insights from one discipline to the real world, we are confronted with validity errors. But rarely in daily practice do we realize that the validity of knowledge is also limited to the level or scale at which it is gained (see Fig. 20.2). In information science—as well as in management—we usually derive insights from small-scale situations such as a local information system, a small group experiment or a regional pilot.

Thus, we have gained insights into the power of recording data and in management tools, such as time schedules and budgets. If we transpose such insights to large-scale situations without checking (at that level) the validity of underlying assumptions, we often make a ‘fallacy of the wrong level’. This might partly explain why so many policy measures and large-scale systems unexpectedly produce poor results—or may even backfire.

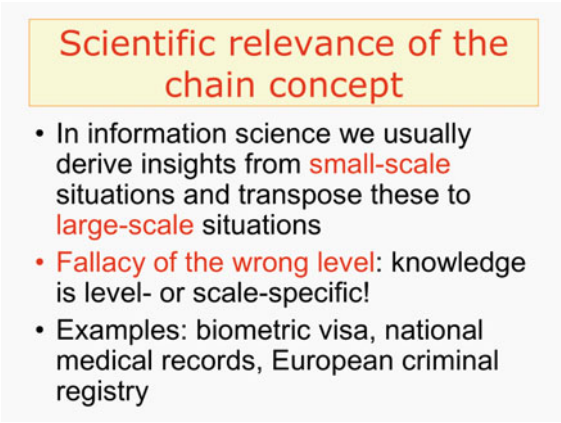

Fig. 20.2 The chain concept safeguarding against fallacies of the wrong level

20.2.5 Example: The European Union's Biometric Visa System

Recently, biometrics has been added to the EU visa system to prevent unwanted foreigners from coming to the European Union. The term biometrics refers to the recognition of a person by a biological and behavioral characteristic such as the imprint of a finger or the pattern of an iris. Information technology makes it possible to quickly digitize a live biological and behavioral characteristic and to compare it, on the fly, with a previously stored specimen. Biometrics is regarded as a more precise way of recognizing individuals than using only administrative details that are not physically linked to the person involved. Thus, the Dutch embassy in the foreign country takes the traveller's fingerprints which are then sent to the Netherlands. If those fingerprints correspond—in the European database—to the fingerprints of unwanted foreigners, then the visa is refused.

On a small-scale, biometrics is considered as an effective instrument for accomplishing this recognition. But will biometrics prove to be as effective when used on a global scale? Consider this scenario: a criminal network needs to send someone to the Netherlands. Suppose that the visa is refused because his fingerprints are in the EU database of unwanted foreigners. Because of this refusal of the visa, the network knows that it has to send someone else or choose a route where traffic control is weak. This means that, instead of the expected greater control of incoming passenger traffic, the arrival of unwanted foreigners will now go largely unnoticed. Thus, the overall result of the biometric visa system is that we put an unnecessary burden on welcome visitors and lose sight of the unwanted foreigners who were the prime target of the system. In this scenario, biometrics applied on a global scale in a visa system is counterproductive. This example demonstrates how easily a fallacy of the wrong level is made, unless we take into account plausible counter-scenarios when designing or building large-scale systems. The larger the scale of a system, the more sophisticated and numerous the checks and balances should be and the smaller the steps to be taken in the process of implementing it. Only a gradual approach, a modest policy measure or a very selective

information exchange has any chance of success in a large-scale environment without coordinating authority.

20.2.6 Remedies Offered by the Doctrine of Chain Computerization

The doctrine of chain–computerization offers several remedies against making fallacies of the wrong level while taking into account the needs and preconditions of large-scale chain cooperation. One such remedy could be, for instance, taking a gradual approach to the development and implementation of large-scale systems. Most of all, we must stop treating large-scale communication systems as intra-organizational information systems with a somewhat larger group of users. This is a classic fallacy of the wrong level. Chain–computerization features a chain approach providing professionals and researchers with a compass that is better suited for a working environment without a coordinating and enforcing authority. This chain approach consists of three components:

1. A model of irrational decision-making (often referred to as the Cohen, March and Olsen (Cohen et al. 1972, March et al. 1976) Garbage Can model)—Chain computerization takes the lack of an overall coordinating and enforcing authority as its starting point. Large databases containing substantive data to be used by many independent organizations call for more authority and willingness to cooperate and pool resources than are usually present in chains, even if every chain partner acts as rationally as possible. Collective decision-making is chaotic and unpredictable. A simple alert mechanism is often the maximum result that can be attained.
2. Dominant chain problem as a focus—Large-scale chain communication systems can only be maintained if focused on a chain problem that creates an interplay of forces strong enough to trigger large-scale inter-organizational collaboration. A dominant chain problem undermines the efforts of every chain partner while no chain partner is able to solve it on its own. In a barely-manageable chain environment, success depends on focus and selection. The dominant chain problem provides this. However, by focusing on the dominant chain problem alone, other problems in the chain are not addressed. Nonetheless, if any problem has a chance of being tackled adequately, it will be the dominant chain problem. If large-scale cooperation aimed at solving the dominant chain problem does not produce adequate support or results, efforts to solve minor (chain) problems will only be of marginal interest.
3. The chain concept is seen as a multi-level concept—The doctrine of chain computerization sees a chain as a multi-level concept (see Fig. 20.3). We can now make a distinction between chain information systems at ‘chain level,’ on the one hand, and intra-organizational information systems that can be linked to a chain information system at the ‘base level’ of the chain, on the other. A chain information system automatically detects which intra-organizational system

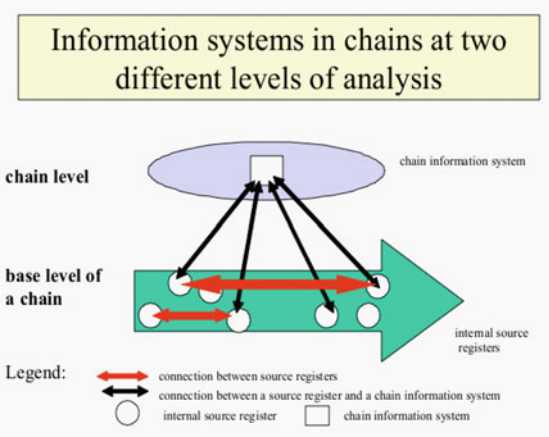

Fig. 20.3 The chain as a multi-level concept

relevant information can be found or, for instance, which organization should be informed. This chain communication is brought about even when chain partners themselves do not know which organizations are involved in the case at hand.

This distinction—for a better understanding of the problems inherent in large-scale cooperation and communication—can be applied on any large-scale phenomenon. To illustrate the analytic value of this distinction, let us consider the common belief that even international chain cooperation could be effectively supported by a single database, containing all the relevant information for every chain partner. At this enormous scale, that yields, little more than a concentration of management activities, not communication. Moreover, that management must be carried out by people who have barely any affinity with the registered details and have no authority to enforce cooperation. Analytically, this chain database can be positioned at chain level, which tells us immediately that content, quality, and use of the data cannot be sufficiently managed because overall coordination and authority do not exist at that level. Therefore, it is much better if every chain partner collects and manages its own information. Analytically, this can be seen as occurring at the base level of the chain where chain partners behave as rationally as they can and are supposed to support their work processes in their best interests. This is precisely an important precondition for high quality information management.

20.2.7 Chain Research Results in the Chain Dimension

The chain research program offers some interesting results in the chain dimension.

- Chain partners look at chain problems solely from the viewpoint of their own organization, interests, and priorities. Every chain partner oversees only part of the problem that causes the chain as a whole to be disrupted. Thus, they overestimate their chances and opportunities in the large-scale chain environment and underestimate their risks and difficulties. This might be one of the main factors that

cause big projects and systems to get out of hand or fail to produce the intended results. In our chain research, we were thus confronted with the problem that dominant chain problems cannot be found by interviewing chain partners and counting the responses. We had to perform a disciplined analysis to discover if there was a chain problem and to then assess its dominant character.

- Dominant chain problems differ greatly and therefore, require a chain-specific information infrastructure. This results in a great variety of public information infrastructures and chain relations among the organizations, and professionals involved.
- Sixteen out of the twenty chains studied, thus far, proved to pivot upon the identity of the person or object involved though in different ways, depending on the dominant chain problem. Moreover, in four out of these sixteen chains, identity fraud was at the core of the dominant chain.
- In complex chain processes, the processing of cases requires closely interlinked feed forward and feedback mechanisms causing chain communication systems to be absolutely indispensable. But, in seventeen of the twenty chains studied, research indicates that, because of the lack of chain cooperation at the national scale the development of national information-infrastructures will not be feasible (12 chains) or will take another 5–10 years (5 chains). Governments, unfortunately, show a preference for national approaches and systems, even if regional projects and solutions would have better chances of success.

The chain perspective and the results of the chain research program at the University of Utrecht contribute to a more realistic view of the inter-organizational world. This will lead to better information strategies for large-scale information infrastructures supporting national or international chain cooperation.

20.3 Identity Fraud (Identity Theft)

Before turning to the national criminal law enforcement chain and its European extension, the EU exchange of criminal verdicts, we need to take a closer look at the phenomenon of identity fraud that is gradually undermining many large-scale social systems (Grijpink 2004a).[1] The chain perspective has provided a better understanding of the problem of identity fraud because, in an information society, its real damage will be the disruption of important large-scale communication systems.

20.3.1 The Concept of Identity Fraud (Identity Theft)

Identity fraud—using or stealing somebody else's identity with malicious intent—is becoming a major issue in our information society. The identity fraudster can

[1] See also: Grijpink 2004b.

make use of other people's identity documents or personal numbers, although photos, actions or events can be used as well because they all feature an identity suggestion from which people draw conclusions about whom they are dealing with. Therefore, identity fraud can take place anywhere and in many ways and is not restricted to specific situations, procedures or documents. Once a person has fraudulently changed his identity, the new 'identity' can affect other situations along regular channels. In these situations, it usually is no longer possible to see through the preceding fraudulent identity change. The real problem is that if an identity fraud succeeds, all clues and traces lead to the victim instead of the culprit. This victim subsequently has much difficulty proving his innocence. Thus far, we lack effective institutions, methods, professionals, and powers that enable us to quickly investigate a case of identity fraud—accurately distinguishing between honest victims and pretending culprits—and to initiate appropriate action. Thus, identity fraud forms a major challenge.

20.3.2 Identity Fraud, a Growing Problem

Identity fraud is not a new phenomenon, but the increasing digitization in our mobile and anonymous society gives identity fraud three dimensions that boost its impact and frustrate fighting it.

20.3.2.1 More Traces, Less Evidence

In a digital world, our transactions leave an increasing number of digital—and non-digital—traces, but in case of identity fraud, they always point to the victim instead of the culprit. Therefore, if a case of identity fraud is reported to the police, the victim is seen as the prime suspect. He has to prove that he is not the culprit. That is often difficult because, for example, if a person's internet address has been misused by somebody else, the traces will point to the victim. If one succeeds in misusing somebody else's social security number when starting in a new job, the victim has to pay the taxes. If one succeeds in registering a car on somebody else's name, duties, fines, and collections are presented to the victim instead of the car owner. Regardless of the victim's protestations, government agencies maintain their suspicions that the traces point to the culprit even if they, in turn, are unable to prove this.

20.3.2.2 Identity Fraud Spreading Unnoticed

Successful identity fraud committed in a weak spot of a process easily spreads to other social sectors. If one succeeds in using somebody else's health care number, one can also get medical treatment without being entitled to it. Moreover, the

culprit's medical data are stored in the file of the official holder of the health care number without his being aware of the contamination of his medical file until a medical error occurs that can be traced to incorrect data in somebody's medical file. This way, identity fraud spreads unnoticed into the tiniest capillaries of processes where it cannot be detected any more.

20.3.2.3 Balance of Power Shift in a Digitized Environment

One characteristic of identity fraud that is still rarely taken into account relates to a shift in the balance of power between the person who must check someone's identity and the person being checked. Traditionally the checker is the boss: he takes initiatives whereupon the person to be checked has to react. In digitized procedures—and when digital equipment is being used—the person to be checked is the boss. The average ID checker does not understand how the equipment works and has to rely on the results of the electronic verification. Manipulation of equipment or procedure cannot usually be detected by the checking official. Furthermore, the initiative shifts to the fraudster who can easily initiate an exception procedure, for instance by reporting the loss of a token. Digital ID-checking can be inconspicuously disabled by the person to be checked, thus initiating a fallback procedure, which is generally sloppy. Thus, the element of surprise is on the fraudster's side; it is the checker who has to react while he can never be certain that the problem is being created intentionally. Moreover, in most cases—and by default—the ID checker must rely on unverified or unverifiable information presented to him on the spot by the person to be checked.

20.3.2.4 ID-Checking Involves Blind Spots

We trust administrative identities, even if based on unverified or unverifiable personal data. Moreover, our favorite name-number verification using an ID-document always succeeds, no matter who is making use of it: the information systems containing the identifying details generally are the same systems that have been used in producing the ID-document. Finally, governments prefer general and compulsory use of uniform standard ID-documents, personal numbers, techniques and procedures, thus creating high value and provoking attack!

Identity fraud is difficult to detect while it is taking place unless special tools and procedures are installed. If successful, the victim usually becomes aware of it too late and the culprit cannot be found because all traces point to the victim. In future, identity fraud will keep growing and police investigation will, to an increasing degree, end in unsolvable cases or lead to convicting innocent people. Given the gradual disruption of social systems as a result of identity fraud, prevention really is the only effective strategy and urgently needed because the correction of contaminated files is often impossible. Therefore, ID-checking should become smarter. The test of any system or measure should be: can

identified fraud be prevented or detected? Moreover, better protection of personal data that can be used to construct (or reconstruct) identities is needed.

20.3.3 Chain Research Results in the Identity Fraud Dimension

In the identity dimension, our research suggests some interesting results.

- Because the majority of chains pivot upon the identity of the person or object involved in different ways, depending upon the dominant chain problem, identity management and ID-checking have proven to be chain-specific. This causes general ID-instruments to be vulnerable to attack in weaker chains. Successful identity fraud surreptitiously spreads to other chains, eluding stronger ID-management systems.
- Identity fraud/theft is easy and very profitable. The main reason is that our social systems are not designed to prevent or detect identity fraud/theft. Moreover, the interests and motivations of the target persons in a chain process vary greatly, depending on the dominant chain problem. Because committing identity fraud is not a seriously sanctioned criminal offense, the culprit can effectively evade such unpleasant consequences as long-term imprisonment. Often, the cost-benefit relationship is in his favor.

20.4 Identity Fraud in the Criminal Law Enforcement Chain

We can now combine chain thinking with a clear understanding of identity fraud to look at the Dutch criminal law enforcement chain and its international extension involving EU-exchange of criminal verdicts.

20.4.1 Identity Fraud in the Dutch Criminal Law Enforcement Chain

Because successful identity fraud cannot be easily detected and mostly goes unnoticed, only rarely can a successful fraudster be detected because he is still there. One such situation is the prison cell. If a criminal finds someone willing to sit out his sentence in his place, we find his stand-in person in the cell. If he is unmasked, he must be sent home because serving a sentence in a criminal's place is not a serious crime. In the meantime, the criminal has often been able to disappear. Alternatively, if the criminal has been successful in using the identity of someone else, we find the right person in the cell but with an identity that is not his own. If this identity fraud goes undetected, the criminal is untraceable after his release

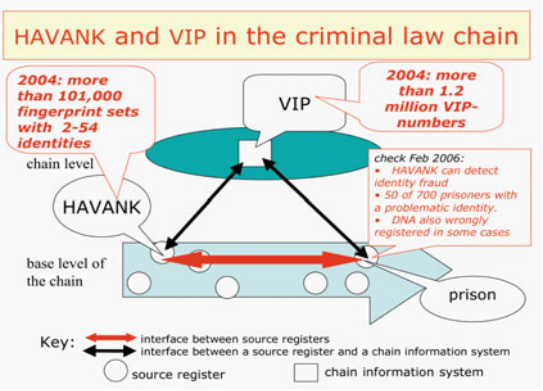

Fig. 20.4 Identity fraud in the criminal law enforcement chain in 2004

because the administrative details of the verdict—stored in the criminal registry for later use—point to someone else.

This scenario could explain how a moral delinquent sometimes succeeds in pursuing his career with a clean slate without links to his previous aliases.

In 2004, more than 100,000 sets of criminal fingerprints linked to more than one administrative identity had been registered in the Dutch national forensic biometrics system HAVANK (see Fig. 20.4). The cleverest criminals had succeeded in using more than 50 aliases, implying that they had managed to get their criminal verdicts spread to as many criminal records of other persons (who may not be aware of it). This volume of aliases was the result of only 15 years of automatic biometric fingerprint checking in only some criminal cases because until October 2010, the Dutch Criminal Procedure Law only allowed the use of forensic biometrics if necessary to prove someone's involvement in the criminal case at hand. An immediate confession thus prevented biometric identity checking. Moreover, note that the volume of identity fraud may be even bigger because a fingerprint set linked to a single name, does not guarantee that this name actually belongs to the criminal.

To understand how this can happen, let us consider some possible scenarios in the first and the fourth links of the chain (see Fig. 20.5):

(A) The first link of the chain: the process of checking the identity of a criminal by the police—in daily practice, the police seem to forget that criminals are not very keen on cooperating. Until October 2010—according to Dutch criminal procedural law—an immediate confession forbade biometric identity checking as it was not necessary to prove the suspect's involvement in the crime at hand.[2] If, in the next stage of the prosecution, the suspect withdraws his confession, the process of identity checking is only rarely restarted from the beginning. Eventually, this causes a criminal verdict to be wrongly filed in the criminal registry. This might be in the file

[2] In October 2010, the law has been changed on this point; biometrical ID checking, done before checking any administrative detail, is now for serious crimes.

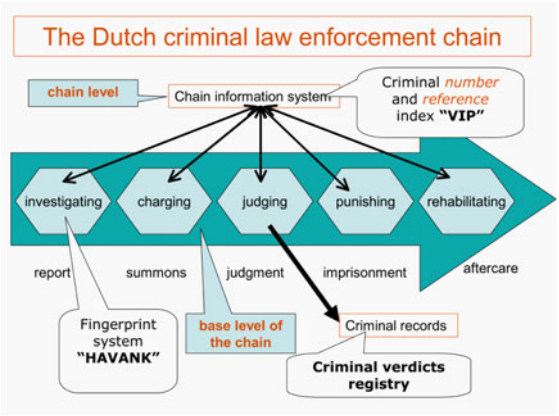

Fig. 20.5 The five links of the criminal law enforcement chain

of the criminal's henchman who then later reports to the prison to serve the sentence on behalf of his sponsor. It might also be the file of an innocent or fictional person.

In other cases, the police will ask for name and address which are then checked against the residents' register of the relevant municipality. (It must be noted that, in 70% of the cases, a suspect cannot produce an ID document). However, if name and address go together, but belong to another person, this checking causes a wrong name mentioned in the official report as well as in the subsequent summons and criminal verdict. Even if the suspect produces an ID, it might be somebody else's. Many people look quite similar and very few people can accurately compare a tiny vague ID photo with a 3D face in front of them, even if they are trained to do so.

(B) The fourth link of the chain: the process of ID checking in prisons—The chain information system—VIP—consists of a personal criminal number (the VIP-number) and a set of references pointing to criminal law enforcement agencies actually involved in this person's criminal justice procedures. The VIP-number is issued to a criminal when he is registered in the information system of one of the chain partners for the first time; it will never be re-issued to another person and will be used at every new contact with one of the chain partners during the rest of his life. Until October 2010, there was no infrastructure enabling prison managers to biometrically check who reports to the prison to undergo his punishment. Until then, the detention process is supported by the purely administrative chain information system,VIP, that can only oversee the chain's efforts at an administrative level. However, from October 2010 onwards, the chain information system VIP is able to detect aliases using the HAVANK-number of the person, his biometrical personal number added to the administrative VIP number. At every new contact, the chain information system immediately warns the chain partner involved of a mistaken identity. In every new case, the criminal file contains a document with the suspect's fingerprint set and two high resolution photographs (front and profile)

taken right at the start of the criminal procedure, at the same time as the enrollment of the fingerprints. Subsequently, we are only left with the challenge of ensuring that older verdicts have been booked under the right name.

Figure 20.4 also shows that, by 2004, the VIP system at chain level had already issued more than 1.2 million VIP-numbers since the system was introduced in 1993. This number of VIP-numbers suggested serious identity problems because the Dutch population could not reasonably provide for so many criminals. In February 2006, the identity of every prisoner in a big multi-prison site with 700 prisoners was thoroughly checked using the forensic biometrics available in the HAVANK system. This involved a huge logistical operation, which required 4 months lead time and could not possibly be kept secret. But, despite the long preparation time that offered many opportunities to evade the biometric checking, some 50 prisoners were found not to be using their own name or not to be the right person. In some cases, DNA data were registered under the false name, as well. This will cause the arrest of the wrong person in a new criminal case and the real criminal being permanently excluded from police investigation.

20.4.2 Identity Fraud in the Criminal Law Enforcement Chain at EU Level

Let us now see how extending the scale of the criminal law enforcement chain from national to international complicates our national approach. International cooperation among national police forces has a long and fruitful tradition, but many other chain partners from other links of the chain—from investigation to rehabilitation—have only incidentally joined. Within the European Union, this chain cooperation takes place within the realm of intergovernmental cooperation. The difficulties that make national chain processes barely-manageable *a fortiori* hold for the European situation.

Fourniret's case (see Fig. 20.6) provides a nice example for understanding the disruptive forces of identity fraud at this level, because it covers two EU member

The Fourniret Case
Michel Fourniret, a French lumberjack, was arrested in 2003 in Belgium because of a failed attempt to abduct a 13-year old girl. Accused by his wife in 2004, he admitted having abducted, raped and murdered eight girls and young women. He had been living in Belgium since 1989, but committed all but one of his crimes in France. Before moving to Belgium he was imprisoned several times in France, for the last time in 1987 when he was given a 5 year sentence because of having raped eleven girls. He was released that same year and placed under police surveillance.
By moving to Belgium in 1989 he was able to shake off his criminal record and to continue there with an apparently clean slate. He even managed to find a job as a handyman at a school in the Belgian village of Sart-Custinne. The Belgian authorities were, allegedly, not aware of his French criminal record. In January 2006 Fourniret was extradited to France to be prosecuted and convicted in France.

Fig. 20.6 Fourniret's case triggering an EU criminal registry

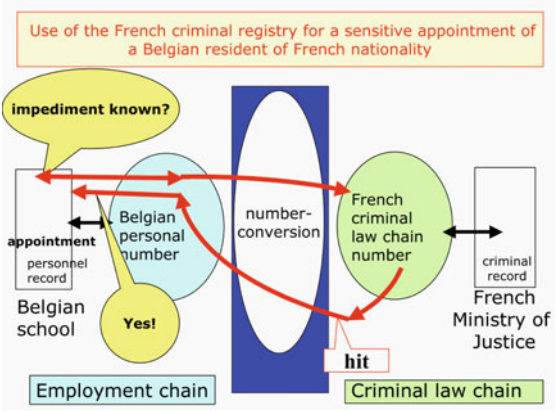

Fig. 20.7 Use of criminal verdict information between two member states

states and also involves communication between the criminal law enforcement chain and two other chains outside the criminal justice domain (Grijpink 2005a, Grijpink 2005b). Previously, information exchange concerning nationals of other member states was only done if and when it was considered necessary for the case at hand.

Thus, apparently, the Belgian police never questioned the French criminal registry during Fourniret's failed abduction investigation. The Belgian education chain might have questioned the Belgian criminal registry because, in many EU member states, Fourniret's job was considered sensitive enough to ask a job candidate for a so-called declaration of good conduct. Thus, consulting the Belgium criminal registry from the Belgian education chain would wrongly have produced a clean slate.

Figure 20.7 shows, how criminal verdict information must be exchanged between two member states at the moment of a sensitive appointment regarding a French national who lives in Belgium. Fourniret's case illustrates how complicated this information exchange is at the EU level. This communication will only be correct if two conditions are met.

- The national criminal law enforcement chain in every member state prevents identity fraud in its own criminal procedures.
- The member state sends every criminal verdict to the member state of which the criminal has the nationality while, at the same time, preventing identity fraud during this transfer.

When these conditions are met, the Belgian school can effectively request information from the Belgian criminal registry in order to make sure that a resident of French nationality in Belgium has no criminal record that could be an impediment for an appointment in Belgium.

Note that, in this example, even then another challenging communication problem must be solved in every member state because two large-scale communication systems concerning criminal verdicts are involved:

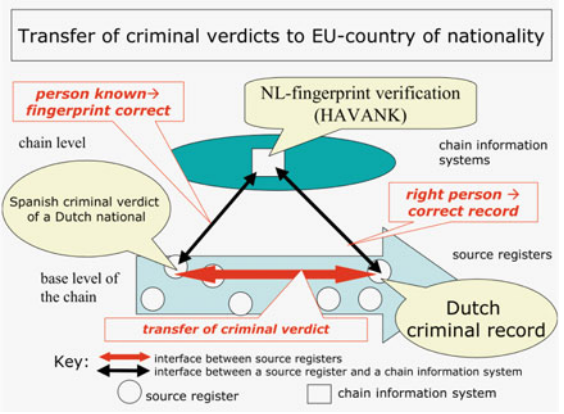

Fig. 20.8 Transfer of criminal verdicts between EU member states

- Within every national criminal law enforcement chain, each new criminal verdict is to be stored in the correct criminal record.
- If the law permits, information about the correct criminal record must be exchanged between the national criminal law chain and any other national chain such as, in this example, the employment chain.

As Fig. 20.8 shows, this implies a close cooperation among police forces within the EU focused on the ID check of their nationals in other EU-countries, using its own forensic biometrics.

We are very far from this ideal situation, but much will already be gained if every transferred criminal verdict is accompanied by a document containing the convicted person's fingerprint set and two high resolution photographs (front and profile) taken right at the start of the criminal procedure and at the same time as the enrollment of the fingerprints. If this document is missing, the criminal verdict should not be filed in the criminal registry of the criminal's member state.

We have seen that only preventive measures can protect against identity fraud. These examples illustrate that the chain concept is a powerful tool in understanding how large-scale public information infrastructures can effectively tackle identity fraud, even on an enormous scale. Politicians and public managers like to simplify this type of complicated interdependence between and within large-scale systems, but our chain research has taught us that this is fruitless. We had better deal with the world as it really is. This does not exclude a simple solution, as these two examples show. At the outbreak of the Fourniret affair, the European Council wished to bring about a single collective criminal registry (Grijpink 2006). Chain computerization theory tells us that a physically centralized EU criminal registry cannot be expected to work adequately at this enormous scale, covering the national criminal law enforcement chains of 27 member states. Fortunately, at the moment, the efforts are being aimed at a bilateral exchange of criminal verdicts regarding member states national, based on a central access system. Eventually, this will lead to a distributed EU criminal registry, in line with the theory of chain

computerization that might be able to prevent criminal cases such as Fourniret's from happening again.

20.5 Some Conclusions and Challenges

20.5.1 Conclusions

We know precious little about large-scale information exchange. We should opt for a gradual approach and for lean and flexible chain communication systems. Chain computerization theory tells us that a physically centralized chain database cannot be expected to work adequately at a national or international scale.

Identity fraud calls for a different identity policy, forcing us to take a fresh look at the parameters, function, and use of identity instruments in our legal culture. It often turns out that measures and instruments that are useful in combating document fraud do not provide solutions that effectively prevent identity fraud. Often they even have the opposite effect.

If criminals succeed in using aliases in the criminal law enforcement chain, criminal records are at fault, and the agreed EU criminal registry will not prevent criminals from continuing their crimes, undetected after moving to another EU member state. This means a growing stream of alias convictions will be added to wrong criminal records, thus disrupting important national chain communication systems that aim at the protection of sensitive jobs and processes. An EU wide information infrastructure featuring remote forensic fingerprint verification from or in the country of nationality is, therefore, an absolute necessity.

The example of the criminal law enforcement chain also applies to many other large systems at EU scale. If it proves to be that easy to use other people's identity under the watchful guard of the criminal law enforcement officials, we must not delude ourselves about the future of identity fraud in less well-guarded public information infrastructures, such as health care, employment, education or travel. If, in future, we are not able to adequately counteract identity fraud—even, for example, in large-scale EU cooperation in the fields of identity management or health care—governments will ultimately lose much of their legitimacy.

20.5.2 Challenges

Politicians and public managers like to simplify the complicated interdependence among and within large-scale chains. Many chain issues tend to provoke a quest for a large chain database. Chain computerization theory tells us that such a physically centralized chain database cannot be expected to work adequately at such a large scale, but how can we prevent them from this awkward reflex?

Smart ID-checking for preventing identity fraud, is an important challenge. This means better strategies on four aspects of every ID checking process.

1. Focus on the person, not only on the ID-document! Strategy: make it difficult to take a free-ride on somebody else's identity.
2. Focus on the process of identity checking in its particular context (e.g., airport, city hall, bank, or police). Strategy: variation in the process makes the success of identity fraud less predictable!
3. Focus on checking data. Strategy: checking data should be independent of the person to be checked which implies that critical data should not be mentioned on ID-documents.
4. Diminish the economic and social value of ID-documents and personal numbers! Strategy: apply additional thresholds (pin code, transaction code, etc): 'knocking three times or more'.

An EU communication system surrounding criminal convictions—based on the country of nationality—that is up to prevent identity fraud, is a major challenge. Much will already be gained if every transferred criminal verdict is accompanied by a document containing the convicted person's fingerprint set and two high resolution photographs (front and profile) taken right at the start of the criminal procedure and at the same time as the enrollment of the fingerprints. If this document is missing, the criminal verdict should not be filed in the criminal registry of the criminal's member state.

If we succeed in developing identity-fraud-resistant public information infrastructures for criminal records, identity records, and health care files, we are left with enormous challenges to ensure that older records and files in these social systems have been registered under the correct name and contain only data concerning the correct person.

References

Cohen MD, March JG, Olsen JP (1972) A garbage can model of organizational choice. Adm Sci Quart 17(1):1–25

Grijpink JHAM (2004a) Identity fraud as a challenge to the constitutional state. Computer Law and Security Report 20(1):29–36. Elsevier Science Ltd, Oxford

Grijpink JHAM (2004b) Two barriers to realizing the benefits of biometrics: A chain vision on biometrics, and identity fraud as biometrics' real challenge. In: Renesse RL van (ed) Optical Security and Counterfeit Deterrence Techniques V. Proceedings of SPIE-IS and T Electronic Imaging, SPIE 5310:90–102

Grijpink JHAM (2005a) Our emerging information society, the challenge of large-scale information exchange in the constitutional state, inaugural address. Utrecht University, Jan 2005, www.cs.uu.nl/people/grijpink/publications

Grijpink JHAM (2005b) Our emerging information society, the challenge of large-scale information exchange in the constitutional state. Computer Law and Security Report 21 (4):328–337. Elsevier Science Ltd, Oxford

Grijpink JHAM (2006) Criminal Records in the European Union, the challenge of large-scale information exchange. European Journal of Crime, Criminal Law and Criminal Justice

14 (1):1–19, Brill Academic Publishers, Leiden. Later also published in: Proceedings of the First International Conference on Legal, Security and Privacy Issues in IT Law (LSPI), part I, Complex nr. 3/2006. Institutt for rettsinformatikk, Oslo, pp 283–303

March JG, Olsen JP et al (1976) Ambiguity and choice in organizations. Bergen, Norway

Miller SJ, Hickson DJ, Wilson DC (1996) Decision-making in organizations. In: Clegg SR, Hardy C, Nord WR (eds) Handbook of Organization Studies. London, Sage

Chapter 21
Access to Law in Europe

Laurens Mommers

Abbreviations

DCA	Dutch Copyright Act
ECRM	Europese Conventie voor de Rechten van de Mens
Gw	Grondwet [Dutch constitution]

Contents

21.1 Introduction 384
21.2 Access to Law in Europe 385
21.2.1 Access to Legal Information at the Dawn of the Internet Age 385
21.2.2 Access to Legal Information from 1999 386
21.2.3 A Case Study: The Netherlands 387
21.3 A Right of Access to Legal Information 389
21.3.1 Levels of Accessibility 389
21.3.2 Accessibility of EUR-Lex 390
21.3.3 Accessibility of Officielebekendmakingen.nl 391
21.3.4 Legal Framework for a Right of Access 392
21.4 Conclusion 397
References 397

Contribution received in 2010.

L. Mommers (✉)
Consultant at Legal Intelligence, Leiden, The Netherlands
e-mail: lmommers@legalintelligence.com

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_21,

21.1 Introduction

Public sector information, more specifically legal information regarding European and national jurisdictions, has become both a commercial asset and an important cornerstone of democratic participation and access to the legal system. This has been recognized by the European Community, resulting in several initiatives, among which a Directive on reuse of public sector information.[1] Reuse of public sector information is related to a wider range of objectives of the Commission concerning, e.g., the delivery of pan-European e-Government services to public administrations, businesses, and citizens.[2]

In this contribution, I will focus on reuse of legal information (a subset of public sector information), and the degree to which actual reuse is successful in establishing added economic value, participation and legal access, the corner stones of EU information reuse policy. I will do this on the basis of an assessment of European policies in the area, the way in which The Netherlands have implemented these, and the practice of legal information reuse in Europe and in The Netherlands.[3]

The online availability of legal information, including primary legal sources such as official gazettes, can be regarded as an important asset of e-Government, as this type of information may improve transparency and accessibility of government. In practice, online availability of primary sources has brought citizens and professionals an easy way of obtaining these sources free of charge, as opposed to using expensive providers of professional information, consulting specialists or having to visit a public library.

There are also serious limits to the actual meaning of online availability of primary legal sources. Not only are important parts of the complete body of information still lacking, the actual impact of availability of primary sources for non-professional publics is limited. This is due to the poor understandability of such sources for these publics.

In this contribution, I will discuss two main dimensions of legal information reuse in The Netherlands and the European Union. First, I will consider the practical interpretation of reuse legislation. Second, I will reflect on the meaning of information reuse practice for a right to access to legal information. The main question to be answered in this contribution is therefore:

---

[1] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the reuse of public sector information, OJ L 345/90, 31/12/2003.

[2] Communication from the Commission to the European Parliament and the Council, Final evaluation of the implementation of the IDABC programme, Brussels, 29/5/2009, COM (2009) 247 final.

[3] As a personal note, I should add that I am closely involved in legal information reuse in the Netherlands, so the knowledge presented in this article is not only derived from my scientific research, but also from my work as a consultant in a firm offering a paid subscription service to legal content, and a free legal search engine, both including content from public sources (www.legalintelligence.com and www.liigl.nl).

Can a right of access to legal information be construed from the current legislative framework applicable to legal information?

21.2 Access to Law in Europe

The Directive on reuse of public sector information[4] marks the start of Europe-wide government information reuse. Although the directive has been issued in 2003, and was implemented in Dutch legislation in 2006,[5] reuse practice shows several obstacles to both commercial parties and citizens wishing to obtain access to legal information.

The evaluation of the Directive on reuse of public sector information was published in 2009.[6] It starts by stressing the importance of public sector information, stating a market value of 27 billion euro, and the progress that has been made in reaching the full potential of information reuse for the economy, removing barriers such as 'discriminatory practices, monopoly markets and a lack of transparency.'[7] Some reasons given for the lack of reaching the full potential of reuse are: short-term cost recovery for making available information resources, restrictive licensing, granting exclusive rights and the lack of knowledge about the information being available.[8]

Most member states have implemented the reuse directive, although several infringement cases have been opened by the Commission.[9] The Commission itself adopted a decision regulating the reuse of its own documents.[10] In the discussion on exclusive arrangements in different member states, the evaluation states that these have been terminated in The Netherlands. It also states that The Netherlands now only charge marginal costs or less. Regarding legal information, the report states that there have been changes to the way in which information is made publicly available, leading to a market growth of 40% since 2002.[11]

21.2.1 Access to Legal Information at the Dawn of the Internet Age

An excellent case of potential public sector information reuse is found in the vast numbers of collections of legal documents established both on the EU level and on

---

[4] See note 1.

[5] Kamerstukken 30 188, Staatsblad 2006, 25, 19 January 2006.

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Reuse of Public Sector Information—Review of Directive 2003/98/EC, COM (2009) 212 final.

[7] Ibid., p. 2.

[8] Ibid., p. 3.

[9] Ibid., p. 4.

[10] Commission Decision 2006/291/EC, Euratom, OJ L 107, 20/4/2006, p. 38.

[11] Ibid., p. 6.

the level of its member states. The collection of primary and secondary EU legislation forms a very large multi-lingual corpus, usable not only for lawyers, but also for linguists.[12] The national collections of legislation, partly based on EU legislation (because national legislation implements EU legislation), also constitute valuable material for comparative law research.

At the dawn of the internet age, access to legal information was still reserved to those having access to commercial publisher's legal products, either in their professional environment or in public libraries. In The Netherlands, the first person putting law texts on the internet and being sued for it was Pavle Bojkovski.[13] He copied law texts from a cd-rom delivered in a standard student edition, including the margin texts added by the publisher. As the Database directive[14] had not been implemented at the time, database rights could not be claimed by the publisher.

The company did, however, claim copyright, with regard to the margin texts (which were removed by Bojkovski) and copyright protection for non-original writings ('geschriftenbescherming') with respect to the law texts. The latter claim was not honored by the judge. The ruling initiated discussion about the effectiveness of public access to law and the then already present waiver of copyright on law texts and case law.[15]

On the EU level, the European Community had already introduced a paid subscription service called 'Celex,' offering access to Community documents. In addition to the paid subscription service, in 1998, a free internet-based service was introduced under the name EUR-Lex.

21.2.2 Access to Legal Information from 1999

The Dutch government started to make available legal information free of charge already before 2005. This action resulted in a series of government websites, under the general denominator overheid.nl, which offers access to a body of consolidated legislation and official publications. Around the same time, in 1999, the site rechtspraak.nl, introduced by the Judiciary Council ('Raad voor de Rechtspraak'), started to offer a selection of case law free of charge through the internet.

On a European level, Celex was merged with EUR-Lex in the course of 2004 (Bernet and Berteloot 2006). From that time onward, all value-added services concerning the availability online of legal documents offered by the Community have been free of charge. Usage statistics indicate that in 2006, there were 170,000

[12] The presence of aligned corpora of reliably translated texts forms a prerequisite for much of the automated translation research.

[13] Case of *Bojkovski* v. *Koninklijke Vermande B.V.*, Rechtbank Den Haag, 20 March 1998.

[14] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27/3/1996.

[15] Art. 11 Dutch Copyright Act (abbreviated DCA).

visits on average each day (Bernet and Berteloot 2006). A revision of its interface has not changed the essential access model based on document typologies and the use of common denominators from the Eurovoc thesaurus. Its major strengths—excellent bibliographical metadata and exhaustive nature—also constitute its weaknesses: delays in delivering content, difficult to use, and impossible to search without profound knowledge of the EU legal system.

Despite the promise of easy reuse of legal information, the system lacks a simple way of downloading all newly added documents, day by day, a major obstacle to easy reuse. For those willing to pay for document delivery, there is only a weekly update service, for which the (considerable) costs are calculated on a per language basis. This is going to change in the next few years, as a tender has been published for a new version of the EUR-Lex website, including web services for document delivery.[16]

21.2.3 A Case Study: The Netherlands

The actual situation in The Netherlands has been a little bit different from the one sketched in the evaluation report cited earlier in this contribution.[17] This is due to several reasons which are probably related to each other: technical reasons, the choice of implementation party and lack of demand driven design.

Both the free service for supplying Dutch legislation and the one for official publications (mainly parliamentary proceedings) were initially built by a publisher. The same publisher markets commercial services in these fields as well. There is a potential substitution effect between the paid services and the free ones: if persons or institutions do not see added value for the paid services, they may turn to the free ones and the publisher may see its turnover decrease. This situation does not constitute incentives for the publisher to provide an optimal product. So without additional safeguards in the contracting procedure (e.g., very specific functional requirements and technical requirements), there is a risk of unnecessary underperformance of the service.

As an example of such underperformance, some features of these services have been particularly annoying in the context of information reuse. The easiest way of obtaining public sector information is downloading it from government websites—insofar as documents are made available, of course. However, the Dutch official

[16] Cf., http://publications.europa.eu/tenders/our/documents/itt_10233/template_ao_en.htm. A web service is not a web site, but an interface useable by computer programs through the internet, for instance to download information in a structured manner.

[17] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Reuse of Public Sector Information—Review of Directive 2003/98/EC, COM (2009) 212 final.

publications website has been session-based until recently.[18] This meant that (a) it was not possible to make permanent links the content on the site (instead, the reuse provider has to copy all documents and host these themselves); and (b) it was harder to download all content.

Further technical barriers to downloading included slow download speeds and a maximum of 200 search results per query. All these barriers in practice mean that complex scripts have to be written in order to 'harvest' all documents available on the website. The alternative, a customized delivery of data, would cost a considerable amount of money, far more than marginal costs, to be paid to the publisher, not to the government.[19]

As of 1 July 2009, the new Electronic Publications Act ('Wet elektronische bekendmaking') has been enacted. This Act now makes the electronic versions of the official gazettes[20] of the Dutch government official (the paper version is no longer leading). On the website www.elektronischebekendmaking.nl, these gazettes are made available. As a corollary of this new site, parliamentary proceedings, for a period of time, have been made available only through other, more or less, 'unofficial' sites, hampering the availability of official publications through an official channel.

In The Netherlands, the official gazettes are only available digitally from 1995. There is a website with consolidated legislation (www.wetten.nl), with historic versions going back to 2002. Because of the availability of a limited digital archive of official gazettes (from 1995), even with the enactment of the Electronic Publications Act, there is often still no way for citizens and lawyers to know the full set of gazettes establishing the legal norms they have to obey—officially they are not allowed to trust the consolidated versions.

Parliamentary history, i.e., the collection of documents denoting the parliamentary proceedings concerning a legislative dossier, is an important source of information for the interpretation of legislation. The availability of this information suffered from the same problems as mentioned for official gazettes: a limited archive and sub-optimal accessibility. With the introduction of www.officielebekendmakingen.nl, this problem should have been solved, but in fact the availability has become even more confusing than before. Suffice it to say here that it is

[18] On 1 July 2009, the new website came into service officially. However, it did not contain all official publications at the time. The only alternative was to use one of the two session-based websites: parlando.sdu.nl or www.overheid.nl/op. parlando.sdu.nl has been suddenly discontinued as of 6 April 2010, without prior notice.

[19] These figures and factual descriptions are based on the experiences of Legal Intelligence in reusing legal information in The Netherlands.

[20] There are three types of 'official gazettes' in The Netherlands: the 'Staatsblad,' the 'Staatscourant,' and the 'Tractatenblad'.

currently unclear where parliamentary proceedings can be found with proper metadata in order to be able to reuse them easily.[21]

On the basis of this short account of the reuse situation of Dutch primary legal sources, it may be concluded that—although reuse opportunities have improved over the last couple of years—the situation is still not ideal. Because of lack of transparency for certain document types, different sites offering (partly) the same information with different delays, and a lack of digitalization of older documents, there still remains much to be improved.

21.3 A Right of Access to Legal Information

Is there a right of access to legal information, and what does this right entail? In the first part of this section, different conceptualizations of accessibility will be scrutinized: what does it mean for legal information to be accessible? Subsequently, I will subject two actual web sites for government information to closer inspection (EUR-Lex and www.officielebekendmakingen.nl) of their compliance with the three levels of accessibility distinguished. Finally, I will relate the different conceptualizations of accessibility to actual (basic) rights that can be related to a right of access, to find out if a 'basic right' of access to legal information can be construed.

21.3.1 Levels of Accessibility

Accessibility of legal information has many faces, so it is necessary to distinguish between different levels. I distinguish between three such levels.

- Primary accessibility (availability), encompassing the availability of information and the ability to search through it. This type of accessibility can occur in the following variants or combinations thereof: (1) document availability—the data have been stored in a non-computer-'readable' format, e.g., jpeg; this means that the document can be accessed electronically but the text is not searchable; (2) full text availability—the data have to be electronically available in a computer-'readable' format, i.e., e.g., ascii text; (3) immediacy—electronic access has to coincide (as much as possible) with the moment the underlying decision was made; (4) continuity—electronic access has to be permanent, and in so far as it is improved, the improvements have to be 'downwards compatible'; (5) searchable content layer—the contents of the documents have to be stored in such a manner

[21] The archive of parliamentary proceedings from before 1995 is currently being digitalized by a project hosted at the royal library: www.statengeneraaldigitaal.nl. Unfortunately, official gazettes are not part of this project.

that they can be searched; (6) searchable meta information layer—this criterion marks the assignment of meaning to pieces of information by labeling them, which makes searching more 'intelligent,' in that searching can become more specific based on the labels assigned.

- Secondary accessibility (meaning) of sources of law starts with meeting the third criterion for primary accessibility: by way of meta information, meaning can be imposed on certain entities or sections in a document. Also, relations can be imposed within or between documents. Examples are meaningful relations between legislation and case law. The following variants of secondary accessibility are available: (1) internal structure—the structure of the document is made explicit with computer-'readable' labels; (2) external structure—the relations between this document and other documents are made explicit, e.g., whether a law is a transposition of an EC Directive; (3) internal meaning—adding information on the meaning of individual parts of the document; (4) external meaning—adding on the information of the meaning of the document or its constituting parts in relation to other documents.
- Tertiary accessibility (understandability) of sources of law starts with providing a context-dependent translation of the contents of the source, meant to clarify its meaning for a certain target group with a specific knowledge level. This is a considerable step further from 'just' adding metadata; it implies having to restructure and translate information completely, based on an appraisal of background knowledge. Both profound legal knowledge of the specific domain, the target group and the best way of communication with the target group are demanded.[22]

One can classify current legal databases in terms of these three forms of accessibility. I use two sites mentioned above: EUR-Lex, the EU legal database, and www.officiëlebekendmakingen.nl, the Dutch database for official publications, for an example of classifying current reuse of government information in terms of satisfying the different purposes of accessibility.

21.3.2 Accessibility of EUR-Lex

With respect to primary accessibility, most documents in EUR-Lex are available in full text. They are generally not immediately added to the database, because meta information is generated first. This takes several days. Because most documents have to be translated in each of the official European languages, it may sometimes take months before all language versions are available. Both the content layer and the meta information layer are searchable. As EUR-Lex is built in the style of a

[22] For a detailed account of understandability and the translation steps needed for it, cf., Mommers et al. 2009.

traditional library, there is a host of meta information available, including keywords assigned from the Eurovoc thesaurus.

With respect to secondary accessibility, the internal structure of documents in EUR-Lex is not made explicit in the document formats made available to the public. There is, however, a possibility of comparing two language versions, which requires proper outlining and thus implies some form of internal structuring in the system. In the elaborate meta information in EUR-Lex, there is ample room for links to related documents (e.g., corrigenda to legal instruments and national measures transposing EC Directives). The use of thesaurus keywords functions as a form of meaning assignment. Outside EUR-Lex, in services such as Pre-Lex and OEIL, the progress of legislative processes is made visible in websites linking all relevant documents.[23]

Finally, with respect to tertiary accessibility, EUR-Lex does itself not offer access to 'translated' documents, but several other services aim to make primary and secondary law of the EU more accessible. Initiatives include a site containing theme-related summaries of legislation (formerly known as 'Scadplus').[24] Thematic portals are another way of providing access to legal information.[25] In general, these provide general information about policy areas, without referring directly to legal instruments.

21.3.3 Accessibility of Officielebekendmakingen.nl

Officielebekendmakingen.nl is the new Dutch official gazettes websites, as explained above. With respect to primary accessibility, it is currently unclear exactly which set of documents is available on this website. At least all gazettes published from 1 July 2009 are available. As the digital versions of the gazettes are now official, there is no delay between the official publication date and digital availability. At least one mistake was made in publishing content, with unclear consequences.[26]

All documents on Officielebekendmakingen.nl are available in full text, so primary accessibility has been guaranteed, also for metadata. With respect to secondary accessibility, the official documents have been made available in XML-format, potentially giving more opportunities for detailed access on a secondary access level. Metadata in the XML-format concern such information as publication dates, document structure, responsible ministry and links to current

[23] See http://ec.europa.eu/prelex/apcnet.cfm?CL=en and http://www.europarl.europa.eu/oeil/

[24] See http://europa.eu/legislation_summaries/index_en.htm

[25] See http://ec.europa.eu/health-eu/index_en.htm

[26] This case concerns the document 'Terinzagelegging ontwerp "Bestemmingsplan Hollum 2009"', Staatscourant 2009, nr. 11483. If searched for on the site, a completely different document is shown. This has been communicated to the site owner on 25 August 2009, but the problem still persists on 2 May 2010—no revised version of the document has been published.

legislation. This, however, does not apply to parliamentary proceedings, which are—in the weeks following first publication—only made available in PDF-format.

The third level of access has been completely ignored. There is no explanation on the site about the status of the documents whatsoever. This is strange, considering the fact that this new site has been made an integral part of the Overheid.nl (Government.nl) portal, which is meant for use by both citizens and companies. Although the portal site Overheid.nl offers 'catalogues' of products, relating to relevant legislation, this part is not linked to the primary legal sources available through Officielebekendmakingen.nl.

21.3.4 Legal Framework for a Right of Access

Internet access to legal information has been gradually realized over the past years, as can be read in the preceding sections: in the area of primary accessibility of legal information, much has improved over the past decade, and even secondary and tertiary accessibility get some attention in practice. This is partly due to national initiatives of making available legal information, and partly due to the Directive on reuse of public sector information.

There are even several indications pointing toward the existence of a right of access to legal information. In this subsection, I will discuss several existing rights that might be supportive in construing a right of access to legal information, or even a right of accessibility of legal information, and two rights that might hinder such a right, or its exercise. An assumed right of access therefore has a multi-dimensional nature—because it is related to, or even derived from, several acknowledged (basic) rights—and it is potentially in conflict with other rights.

What basic rights constitute a right to access to legal information? First, there is the principle of legality. In penal law, it states that there can be no punishment without a prior legal rule.[27] In administrative law, it amounts to providing boundaries to the government's acts, deriving its power to act from explicitly attributed competences.[28] Although in other areas of law, the principle is usually not formulated as strongly, it still exists as a basic right for citizens in order to be able to anticipate to applicable legislation. The principle is usually defined in an 'ontological' way (a prior legal rule must exist). However, being able to know the legal rule before it is applied is at least as important.[29] This epistemic dimension of the legality principle seems important in establishing a right of access to legal information, especially insofar as this right should transcend primary accessibility.

---

[27] Art. 16 Grondwet (Dutch constitution, abbreviated Gw); Art. 7 ECRM.

[28] There is an extensive literature on the legality principle in Dutch administrative law. Cf., as one example of many, Voermans 2004.

[29] For a discussion of epistemic and ontological dimensions of law, cf., Mommers 2002.

Second, freedom of speech is related to the access right. Freedom of speech can only be practiced to its full potential if the democratic society is sufficiently transparent. The articulation function of, e.g., media and pressure groups and the access of citizens to legal information can be improved, by giving more attention to the way in which legal documents are written and made available.[30] Recent case law from the European Court of Human Rights has established further obligations regarding the access to public sector information, derived from the ECRM article on freedom of speech.[31]

In his note for this decision, Hins (2009) stresses the consequences that this decision might have for Dutch practice, in which, e.g., courts are not within the application of the Government Information Act (Wob). Complainants, he states, try to derive a positive obligation analogous to the interpretation of Article 8 ECRM (privacy) from Article 10 ECRM (freedom of speech), but he stresses that the Court, considering paragraph 35 of its decision, has not reached that point, thus not leading to a full recognition of a right of access to administrative data and documents on the basis of Article 10 ECRM as yet.[32]

Dommering, in his note to the same case, adds that the Court brings the 'right to seek information' under the scope of Article 10 ECRM, insofar as the party concerned functions as a 'social watchdog,' comparable to the press.[33] As imposing 'arbitrary restrictions' by law to the gathering of information can be construed as (indirect) censorship,[34] Article 10 ECRM might play a role in supporting a right of access to legal information.

Third, a right of access to justice has been made explicit for penal cases.[35] According to the European Court of Human Rights, this right also encompasses civil and administrative cases, as became clear from the Kadi and Bosphorus cases.[36] In these cases, the implementation of a sanction regime of the UN Security Council by national jurisdictions or the European Community does not involve a suitable way of challenging these sanctions before a court. Whether the concrete right of bringing a case before a court in these cases implies—or is related to—a

---

[30] Art. 7 para 1 Gw; Art. 10 ECRM.

[31] Cf., European Court of Human Rights, case of *Társaság a Szabadságjogokért* v. *Hungary*, Application No. 37374/05, 14 April 2009, para 35: '…Nevertheless, the Court has recently advanced toward a broader interpretation of the notion of "freedom to receive information" (see Sdru[zcaron]ení Jihoceské Matky c. la République tchèque (dec.), no. 19101/03, 10 July 2006) and thereby toward the recognition of a right of access to information.' See also European Court of Human Rights, case of *Kenedi* v. *Hungary*, Application No. 31475/05, 26 May 2009, paras 40–45.

[32] Cf., the note of A.W. Hins for the decision mentioned in the previous note in European Human Rights Cases (EHRC) 2009/74.

[33] Dommering 2010, note for the decision mentioned in note 30.

[34] Para 27 case of *Társaság a Szabadságjogokért* v. *Hungary* (No. 37374/05, 14 April 2009).

[35] Art. 15 para 2 and Art. 17 Gw; Arts. 6 and 13 ECRM.

[36] ECoJ 3 September 2008, cases C-402/05P & C-415/05P (*Kadi/Al-Barakaat* v. *Council*) and ECHR 2005/91 *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi ('Bosphorus Airways')* v. *Ireland*.

right to information about access to that court is a matter for further legal research. One ECHR decision that is interesting in this respect is the case of *Staroszczyk* v. *Poland*. It states a right to hear the grounds of the refusal to represent a customer, and thereby connects a right to specific legal information to the right of access to justice.[37]

Fourth, transparency of government is acknowledged as principle both on a European and on a national level.[38] In both cases, it is mostly translated into a regime for accessibility of documents. The fact that case law (and sometimes other formal sources of law) is excluded from application of these regulations is not that important, as special regimes apply to them that guarantee a degree of transparency as well. Having access to other documents (e.g., parliamentary proceedings and policy documents) can be relevant in the interpretation of formal sources of law.

As opposed to these rights supportive of a right of access to legal information, two rights might have the power to limit that right of access: privacy and copyright. Privacy protection implies a potential limitation of the right of access.[39] The main source of privacy concerns is case law in which the names of the persons involved are not anonymized, or in which other personal data can be derived from circumstances of the case (cf., De Meij et al. 2006). Kranenborg (2007) has extensively discussed the balancing of privacy rights of individuals mentioned in documents and a right of access to documents containing personal data. An example is the Bavarian case in which an English brewer wanted access to the minutes of a meeting between the European Commission and a trade organization,

[37] Para 135, case of *Staroszczyk* v. *Poland* (No. 59519/00, 22 March 2007) states: 'The Court is further of the view that when examining the circumstances of the present case it must have regard to the specific features of the Polish system of legal aid. In this respect, the Court deems that the refusal of a legal aid lawyer should meet certain quality requirements. In particular, the refusal must not be formulated in such a way as to leave the client in a state of uncertainty as to its legal grounds.'

[38] Cf., Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, pp. 43–48; also cf., the Dutch Government Information (Public Access) Act 1991 ('Wet openbaarheid bestuur' or Wob). Also cf., COM (2008) 229; Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=196983

[39] Art. 10 para 1 Gw; Art. 8 ECHR; for an implementation of the right to privacy in 'normal' (secondary) legislation, cf., Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 pp. 31–50, and the Dutch Privacy Act ('Wet bescherming persoonsgegevens').

but the names of trade organizations' representatives mentioned in those minutes were hidden on the latter's request (Kranenborg 2007).[40]

Copyright protection also implies a potential limitation of the right of access. The most obvious example is the reference to norms issued by private organizations in public legislation. Examples are the reference to norms of The Netherlands Standardization.

Institute. This phenomenon has been subject of elaborate research (Elferink 1998, 2007; Stuurman 2010). Whereas case law and legislation are generally exempted from copyright,[41] the presence of norms issued by privately held institutions, which often have to earn part or whole of their income by issuing regulative documents, leads to problems in the application of access-related norms.[42]

As one of few scholars trying to construe a right of access, Jamar (2001) constructs the human right of access to legal information as a part of the transparency principle, Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights. He uses both the right of access to information (in a broad sense) and the implicit assumption of accessibility in the ICESCR to construct this specific right.

Emphasizing the epistemic dimension of the right of access—defining it as a right to be able to take notice of legal information, to understand it—is vital to provide it with more weight. Having access to documents underlying the law is a necessary but not sufficient condition to fulfill in order to attain a 'material' right of access. To attain such a right, in general the conception of an 'average person' must be determined in order to have a reference for the necessary degree of understandability. I propose—as a provisional, normative step, to be further grounded in relevant legal sources—an extensive interpretation of the legality criterion, taking the epistemic dimension a step further: in order for a legal norm to be a valid one, an average citizen should, under average circumstances, be able to understand that norm.

The 'average citizen' might be partly based on similar concepts in European legislation, e.g., the 'average consumer' that is mentioned in several European directives, defined in the preamble of Directive 2005/25/EC as 'reasonably well-informed and reasonably observant and circumspect, taking into account

[40] See the opinion of advocate-general Sharpston delivered on 15 October 2009, case C-28/08 P, *Commission of the European Communities* v. *The Bavarian Lager Co. Ltd*. and Judgment of the Court of First Instance (Fourth Chamber) of 14 October 1999, *The Bavarian Lager Company Ltd* v. *Commission of the European Communities*, case T-309/97.

[41] Cf., Art. 11 DCA referred to above.

[42] Such as, apart from Art. 11 DCA, the relevant articles (11a–i) in the Government Information (Public Access) Act 1991.

social, cultural and linguistic factors.'[43] However, it is possibly fair to expect a higher degree of observance for a citizen than for a consumer. Both the reception of the 'average consumer' in case law and its relevance for a further analysis of the concept of an 'average citizen' will have to be determined in further research.

Turning the usual ontological 'version' of legality into an epistemic counterpart in which an 'average citizen' functions as a measure for accessibility and understandability means a considerable change in the interpretation of the legality criterion. However, without such an extensive interpretation, the legality criterion is rather empty. Also, I do not propose that each citizen has to be able to comprehend a norm in each situation; there will be many situations in which the help of another person is needed, or where there is not sufficient time for reflection.

Summarizing, in addition to an epistemic interpretation of legality, the rights of freedom of speech, access to justice and transparency provide support for an extensive interpretation of the right of access to legal information in order to stretch it from mere availability to meaningful access and understandability; the second and third levels of accessibility. Neither the right to privacy, nor the protection of copyright, can provide decisive reasons against such an extensive right of access. In balancing the rights of individuals and the value of a transparent legal system, privacy and copyright will find difficulty in prevailing.

However, if current websites containing public sector information or more specifically legal information are assessed from the accessibility criteria—as I have done in Sects. 21.3.2 and 21.3.3 above, it becomes clear that we have a long road ahead in terms of understandability of such information. Not only are there still elements lacking with respect to the primary accessibility (e.g., electronic archives and immediate publication), also the few initiatives in secondary and especially tertiary accessibility leave much to be desired, particularly for those who lack legal expertise. The three levels of accessibility distinguished in Sect. 21.3.1 provide a practical interpretation of the form a right of access—and a right of accessibility—can take in practice.

[43] Cf., the preamble, para 18, of the Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive'), OJ L 149, pp. 22–39, which states: 'this Directive takes as a benchmark the average consumer, who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors, as interpreted by the Court of Justice, but also contains provisions aimed at preventing the exploitation of consumers whose characteristics make them particularly vulnerable to unfair commercial practices,' and Arts. 5 through 8 of this Directive. Cf., also, e.g., Commission Directive 2007/29/EC, preamble para (4), and various European regulations which mention this concept.

21.4 Conclusion

Given the various basic rights pointing into the direction of a right of access to legal information, it is not hard to assume that the right should indeed exist. There is, however, not one decisive basic right which implies its existence, although an epistemic interpretation of the legality criterion provides strong support. Both developments in positive law, such as the development of transparency criteria with respect to government documents, and technological developments, offering more opportunities for improving accessibility, will tend to raise expectations for a basic right of access to legal information.

Not withstanding this observation, the scope of such a right is much harder to establish. As we have seen, the concept of access embodies different levels, for which it is not easy to establish the degree to which it applies to the right of access. In an ideal world, the law would be understandable for anyone, but asking this from the government and the judiciary would be unrealistic. Improving the degree of access on all levels, however, should become part of government policy.

In the light of the main question asked in the introduction to this contribution—can a right of access to legal information be construed from the current legislative framework applicable to legal information?—a careful 'yes' is the answer, but a positive answer only gains weight when especially the second and third types of access are fulfilled to a certain degree. Not only do we need an epistemic interpretation of the legality criterion for this, we also have to determine how such accessibility of legal information can be attained in practice. Although the 'functional' levels of accessibility have been addressed in Sect. 21.3.1, the question how to reach these functional levels is an issue outside the scope of this contribution.[44]

Acknowledgments The author would like to thank the editors for their constructive and useful comments on previous versions of this article.

References

Bernet H, Berteloot P (2006) EUR-Lex: a multilingual online website for European Union law. Int Rev Law Computers Technol 20(3):337–339

Dommering EJ (2010) In: Nederlandse Jurisprudentie 2010/209

Elferink MH (1998) Verwijzingen in wetgeving. Over de publiekrechtelijke en auteursrechtelijke status van normalisatienormen. Kluwer, Deventer

Elferink MH (2007) Auteursrecht op normalisatienormen revisited. In: Visser DJG, Verkade DWF (red) Een eigen oorspronkelijk karakter. Delex, Amsterdam, pp 79–90

Hins W (2009) Note to European Court of Human Rights, Case of Társaság a Szabadságjogokért v. Hungary, Application No 37374/05, 14 April 2009. European Human Rights Cases 2009-7, No 74

[44] Cf., on this issue Mommers et al. 2009.

Jamar SD (2001) The human right of access to legal information: using technology to advance transparency and the rule of law. Glob Jurist Top 1(2):1–13

Kranenborg HR (2007) Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie. Over de openbaarheid van persoonsgegevens [Access to documents and the protection of personal data in the European Union. On public access to personal data]. Kluwer, Deventer, p 351

Meij JM et al (2006) Toegang tot rechterlijke uitspraken. Rapport van de VMC-studiecommissie Openbaarheid van rechtspraak. Mediaforum 4:1–20

Mommers L (2002) Applied legal epistemology. Building a knowledge-based ontology of law. Leiden, PhD thesis

Mommers L et al (2009) Understanding the Law: improving legal knowledge dissemination by translating the contents of formal sources of law. Artificial Intelligence and Law Vol 17. Springer, Netherlands, pp 51–78

Stuurman K (2010) Public access to standards: some fundamental issues and recent developments. In: Mommers et al (eds) Het binnenste buiten. Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout H. J. Schmidt, hoogleraar Recht en Informatica te Leiden. eLaw@Leiden, Leiden, pp 405–415

Voermans WJM (2004) Toedeling van bevoegdheid, rede uitgesproken bij de aanvaarding van het ambt van hoogleraar op het gebied van het staats—en bestuursrecht aan de universiteit Leiden op 12 September 2003. Boom Juridische Uitgevers, Den Haag

Part VI
Legal Dimensions: Law and Philosophy Perspective

Chapter 22
Identity Theft and Fraud

Peter van Schijndel

Contents

22.1 Introduction 402
22.2 A Definition of Identity 403
22.2.1 Locke 403
22.2.2 Internal Identity 405
22.2.3 External Identity 405
22.3 Identification 406
22.3.1 Identifiers 406
22.3.2 Control Over External Identity 407
22.4 Identity Fraud and Theft 408
22.4.1 Switched Identities 408
22.4.2 Motives 409
22.4.3 Means 410
22.4.4 Definitions 410
22.5 Illegality Under Dutch Law 410
22.5.1 Criminal Law—Fraud 411
22.5.2 Criminal Law—Theft 412
22.6 A Recent Case of Identity Theft 413
22.7 Conclusions 415
References 416

Contribution received in 2010.

Peter van Schijndel wrote his master's thesis, at the Centre for eLaw, on the subject of Identity Theft. This chapter is based on Schijndel (2009).

P. van Schijndel (✉)
Hoyng Monegier LLP, Amsterdam, The Netherlands
e-mail: vanschijndelp@hoyngmonegier.com

P. van Schijndel
The Centre for eLaw, Leiden University, Leiden, The Netherlands

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_22,

22.1 Introduction

There are many different forms of identity theft. In 2004, I fell victim to one of the more common ones, debit card fraud. Someone had managed to copy my debit card and had also acquired my pin code. Presumably through a modified ATM, fitted with a card reader and a small hidden camera. Using the copied debit card and spied pin code, this person then managed to empty my entire checking's account at various ATM's abroad, in France and Italy. I had an overdraft facility, and the criminal was more than happy to take full advantage of that as well. Overnight, the little credit I had with the bank was converted into a 1,000 € debt.

Debit card fraud is not an ordinary theft of money. The criminals who took my money did not employ old-fashioned methods. They did not physically pick my pockets, or demand that I hand over my wallet at gunpoint. Neither did they visit the bank under cover of night, nor empty the vaults armed to the teeth. Instead, they walked up to various ATM's in broad daylight. Maybe they even waited patiently in line with other customers. Upon reaching the top of queue, they presented a copy of my debit-card, entered my pin code and withdrew the amount of their choice. And, depending on the make and model of the ATM, the machine may have even greeted them with a cheerful 'Good afternoon Mr. van Schijndel.' No one ever noticed the crime, until I discovered on my monthly statements that my credit had now become a debt.

Debit card fraud is special for another reason. If the criminals I fell victim to had been more traditionally inclined, they would have merely been able to steal the money present in my purse or—if they had paid a visit to the bank—in the bank's vaults. They would however, not have been able to create a debt in my name. The overdraft facility would have remained out of reach.

They were able to take all my money and leave me in debt, because at the time of the crime the bank—or rather its ATM—was of the opinion that it was merely performing its agreement with me: that is, to pay out any balance and to provide a loan at my request. Because the criminal presented a copy of my debit-card and my (spied) pin code, the bank was convinced that the criminal was me, and thus entitled to the balance of my account.

In order to steal my money, and burden me with a debt, the criminal first stole my identity.

In 2004, I had a hard time convincing the bank that I was the victim of a crime. That someone else had withdrawn my money without my permission, and that I had no intention of assuming a debt nor had benefited from that debt. Luckily I was able to prove that I was nowhere near Italy or France at the time of the withdrawals, but that was not enough. The bank was of the opinion that even if I had not personally been in Italy or France, I at least had some involvement in the crime. Although I eventually got my money back, the bank proved very reluctant

to admit that their systems could be wrong.[1] That it was indeed possible that someone else had successfully assumed my virtual identity, and had fooled the machine into handing over my very real money.

Since then years have passed. The reaction of the bank, to trust the machine and—at least at first—deny the possibly of identity theft is however, still common. At the heart of that reaction lays a lack of understanding of the concept, and the mechanisms of identity theft.

To understand identity theft, the object of that theft must first be defined. This chapter establishes a definition for identity. Based on that definition, an analysis is made of the different ways in which identity may be (mis)used, which results in definitions of identity theft and identity fraud. These definitions are used to test whether Dutch law provides adequate remedies against identity theft and fraud. The chapter concludes with an example of an analysis of the governmental and judicial response to that particular case.

22.2 A Definition of Identity

No single generally accepted definition of 'identity' exists in legal literature (Marbus 2009, p. 8). The term is used often, but its meaning must be derived from the context in which it is used. As an example, in one article on the subject, at least five different forms of identity are evident.[2] That makes research on identity theft difficult. Philosophy, unlike Law, has had less trouble in providing solid definitions of 'identity.' John Locke (Locke 1786, Chapter 27) construed a definition of identity that proves remarkably useful in studying today's identity theft.

22.2.1 Locke

Locke's concept of identity is based on the sameness of objects in space and time.

22.2.1.1 Identity

> [W]hen, considering any Thing as existing at any determined Time and Place, we compare it with itself existing at another Time, and thereon form the Ideas of Identity and Diversity. When we see any Thing to be in any Place in any Instant of Time, we are sure

[1] Kuiper 2004, provides some statistical data on the success-rate of claims for reimbursement after debit-card fraud: only 12.16% of all claims were awarded. At present banks are more forthcoming in compensating victims.

[2] Prins 2007, identifies five different forms of identity all dependent on their context: (1) legal identity, (2) administrative identity, (3) cultural identity, (4) religious identity and (5) personal identity.

> (be it what it will) that it is that very Thing, and not another, which at that Time exists in another Place, how like and undistinguishable soever it may be in all other respects: and in this consists Identity, when the Ideas it is attributed to, vary not at all from what they were that Moment wherein we consider their former Existence, and to which we compare the present;

Locke acknowledges that living organisms and dead matter are two different things, and should have different definitions of identity.

> Dead matter loses its identity … if one of [its] Atoms be taken away, or one new one added, it is no longer the same Mass, or the same body.

Living beings however, do not derive their identity from having an immutable mass.

> An Oak growing from a Plant into a Tree, and then lopped, is still the same Oak.

Living beings rather derive their identity from the continuation of life.

> This also shows wherein Identity of the same Man consists, viz. in nothing but a Participation of the same continued Life, by constantly fleeting Particles of Matter, in Succession vitally united to the same organized Body.

Lock makes a further distinction between living organisms and persons, those organisms with the abilities of reason and self-reflection.

22.2.1.2 Persons

> [T]o find wherein personal Identity persists, we must consider what Person stands for; which, I think, is a thinking intelligent Being, that has Reason and Reflection, and can consider itself as itself, the same thinking Thing, in different Times and Places: which it does only by that Consciousness which is inseparable from Thinking, and, as it seems to me, essential to it: it being impossible for anyone to perceive, without perceiving that he does perceive. When we see, hear, smell, taste, feel, meditate, or will any Thing, we know that we do so. Thus it is always as to our present Sensations and Perceptions: And by this every one is to himself that which he calls Self.

Personality is based on an intelligent being's ability to recognize itself in its own thoughts and actions. Personal identity is then the ability to recognize oneself in one's own present and past thoughts and actions. Integrity of consciousness defines personal identity.

22.2.1.3 Personal Identity

> For it is by the Consciousness it has of its present Thoughts and Actions, that it is Self to it Self, and so will be the same Self, as far as the same Consciousness can extend to Actions past, or to come; and would be by Distance of Time, or Change of Substance, no more two Persons, than a Man be two Men, by wearing other Clothes Today than he did Yesterday,

with a long or short Sleep between: the same Consciousness uniting those distant Actions into the same Person, whatever Substances contributes to their Production.

22.2.2 Internal Identity

Locke's concept of identity is internal. It is a set of past and present, thoughts and actions that defines one's identity and is stored in one's consciousness. I refer to this identity as internal identity. Internal identity is by its nature unknown and inaccessible to others. It cannot be stolen.

22.2.3 External Identity

The content of internal identity remains unknown to the outside world. In Locke's day and age, that was not a big problem. People lived in small communities and knew each other well through their daily encounters. Through these encounters people formed their own idea of the identities of the people around them.

Society has changed since then. People no longer live in small communities—and it is not uncommon to move from community to several times during a lifetime. On a daily basis we are in contact, and do business with, people we have never met—and probably never will. Our society has become too large to know people on a personal level (O'Harrow 2005, p. 79).

Several sectors of society have a (perceived) need to be able to know the identity of other people. The state, and its government, is interested in the identities of its subjects for purposes of public administration and law enforcement (Poster 2007, p. 134). This information need of the state is not limited to passive supervision, but extends to active involvement for implementation and execution of the welfare state.[3] Large administrations have been created for these purposes.

Not only the government is interested in personal affairs. The business world is also fascinated by personal knowledge about the members of the public. That is largely a necessity caused by the scale of the current business institutions. They have become too big to know each customer on a personal, and instead rely on client files containing information about their customers (Clarke 1994, pp. 4, 13). In some cases this need is obvious: little doubt exists about the requirement of a hospital to be aware of their patient's medical history. Or that it is preferable that a bank 'remembers' what amounts each of its clients has deposited.

The information needs of the business world, however, do not stop with information about their current clients and contacts; it extends to prospective clients and contacts as well—and by that means to the public at large. Information about personal needs, preferences and socio–economic circumstances are a

[3] Reference is made to Foucalt and his idea of 'Gouvernementalité,' Foucalt 1991, p. 100.

valuable marketing tool. When entering into any contract, personal information about the prospective counter party is considered valuable. Banks use credit-rating agencies to assess the creditworthiness of their prospective clients. Employers have been known to enlist organizations that perform extensive background checks on future employees. The result is a proliferation of recorded personal information, and organizations specialized in collecting and providing it.

Last, but not least, personal information is not only gathered and recorded by the government and businesses, but also by individuals themselves. Social networks such as Facebook, Linked-in, Myspace and Hyves contain vast collections of personal information about the persons that have made a profile for themselves. The information in these profiles is not only provided by the owners of the profiles, but also by their 'friends' and 'connections.'

The administrations form an external counterpart of Locke's internal identity. The administrations perform the same function as our consciousness: meticulously recording all actions that are associated with any given person. Each separate administration may in itself not contain enough information to provide a complete picture of the person it describes—it is not a complete identity. When all information scattered over the separate administrations is combined, however, a rather detailed image presents itself—a complete external identity. Whereas Locke's internal identity is safely tucked away in the consciousness, external identity is contained in administrations; accessible to others.

22.3 Identification

22.3.1 Identifiers

The data stored in various administrations comprises external identities. Some of those identities are entirely virtual, such as avatars in Second Life and other online communities.[4] Many of the external identities will however, refer to a real person. External identities permit the public to 'know' the person that they describe. To do so, a link must first be made between the external identity and the associated person (Poster 2007, p. 135). In this process called identification data is associated with a particular human being (Clarke 1994, pp. 6–37).

A variety of means exist for identifying a person; to make the link between data and person. These means rely on characteristic that specific to the person

[4] An avatar will usually 'belong' to a real person, but may in some cases not be a representation of that person. The owner may not recognize himself in the actions of his avatar: e.g., in the atrocities of war committed by his World of Warcraft avatar. The avatar and the person behind the avatar are in Locke's definition of identity, not the same person. Being the 'owner' of an avatar, and having instructed the avatar, will however be part of the identity of the real person.

observed, and set him apart from the public. Such a characteristic is an 'identifier.' Identifiers can be grouped in four categories[5]:

- Names and codes—or what the person is called by other people and organizations;
- Knowledge—or what the person knows;
- Tokens—or what the person has;
- Bio-metrics—or what the person physically is or does.

All identifiers have their own weaknesses. Names and codes are not very specific, as multiple persons share the same name, and any given code may be used by different organizations for different persons. Knowledge is not always as secret as one might hope. Tokens may be lost. Biometric information may not be reliable, or the process of 'reading' may be unpleasant (and in some cases impossible if someone's physical appearance does not conform to the 'standard').

Not only identifiers have their weaknesses, the processes of identification in which they are used are also vulnerable. In most cases, the reliability of any identification attempt is dependent on the success or integrity of previous identification processes. For example: identification based on a passport relies on successful identification when that passport was first issued. Identification based on fingerprints is reliant on prior successful identification when prints were added to the database. This layered nature not only exist at the level of each identifier, it extends to the creation of those identifiers. For example: a person may be identified on the basis of his driver's license, but it should be noted that the driver's license was issued pursuant to identification on the basis of a passport, issued on the basis of a birth certificate. An error on any level in this chain taints the reliability of the entire identification process. And finally, as identification relies on matching observations with registered data, many identifiers will be known by many persons—not only by the person identified by it. Information to be matched needs to be available on both sides of the match (LoPucki 2001, p. 96).

22.3.2 Control Over External Identity

Identifiers are the key links between persons and their external identities. By using an identifier in the correct identification protocol, persons gain access to and control over external identities. After a successful identification, the past actions—and the rights and obligations—associated with the external identity are imposed on the identified person. External identities thus influence real persons through identifiers. This process also works the other way around. After a person has been identified and linked to an external identity, his current actions will be

[5] The list is a condensed grouping of the examples given in: Clarke 1994.

ascribed to the external identity. Through identifiers persons and external identities influence each other.

22.4 Identity Fraud and Theft

No commonly accepted definitions for identity theft and fraud exist (van der Meulen 2009). Whether 'identity' can be the object of 'theft' is also still open to debate.[6]

22.4.1 Switched Identities

At the core of the identity theft and fraud problem the imperfect link between person and external identities. As shown above, weaknesses in both identifiers and the identification protocols in which they are used may lead to a person being linked to the wrong external identity. These errors may be caused by accident. When an identifier matches multiple persons—or external identities—it becomes unclear which person corresponds to what external identity; two or more identities collide. The error may also be forced intentionally, by exploiting the weaknesses with the intent of forcing a switch of external identities (Solove 2004, p. 18); a person is deliberately linked to an external identity that does not describe himself.[7]

This last category, of intentionally switched identities forms the basis of identity theft and fraud. The category may be further divided in four categories (Rost and Meints 2005, p. 218):

1. Identity takeover: the assumption of an external identity of another person, without that persons consent;
2. Identity delegation: the assumption of an external identity of another person, with that person's consent;
3. Identity swap: the reciprocal and consensual assumption of each others external identities; and
4. Identity creation: the creation and assumption of a new external identity that does not refer to a real person.

Whether or not a particular identity switch is legitimate or illegal depends on the applicable jurisdiction. Notwithstanding differences between jurisdictions, for the first three categories quite universal legitimate and illegal examples can be found. Identity delegation: a credit card holder may lend his card to a relative to go

[6] The possibility is denied in De Vries et al. 2007, p. 219.

[7] See Rost and Meints 2005, p. 217, where the concepts of 'Identitätskolision' and 'Identitätswechsel' are introduced.

shopping, but he may not lend his health-insurance card for her to receive free medical treatment. Identity swap: two persons may choose to switch lives for a day, but a criminal and his accomplice may not do so if the aim is to avoid punishment or incarceration (Grijpink 2005).[8] Identity creation: it is common for writers to publish books under a pseudonym, but it is not accepted for criminals to attribute their work to an alias. It is harder, however, to come up with legal examples of identity takeover.

When referring to identity fraud, I refer to those cases of switched identities that are considered wrongful in the jurisdiction in which they are performed. Identity theft refers to wrongful instances of the first subcategory, identity takeover. In such instances an identity criminal takes control of someone else's identity without their consent—the identity is 'stolen.'

22.4.2 Motives

The ever-increasing role external identities play in our society has created the motive for identity theft and fraud (Koops and Leenes 2006, p. 3). As the external identity has gained more momentum in dictating what rights—and obligations—a person enjoys, assuming someone else's external identity has become lucrative.

There are two distinct motives an identity criminal may have: money and unpunished crime. In the first case, a criminal is interested in exploiting the financial rights associated with the external identity he assumes. This may include emptying bank accounts, as is the case in debit card fraud, but may also entail attracting debt, as is the case with credit card fraud. Identity theft and fraud with a financial motive is generally referred to as 'financial identity theft/fraud' (van der Meulen 2006). The second motive is avoiding prosecution and punishment for committed crimes. By assuming another identity, the criminal avoids that the committed crime is connected to his person; thus reaping the benefits of his crime while avoiding the negative consequences. A variation on the last motive is to be able to commit crimes that require a certain specific identity, for instance the assumption of the identity of an employee of an airport in order to be able to enter areas closed off to the public. Identity theft with the purpose of criminal acts other than financial gain is usually referred to as 'criminal identity theft/fraud.'[9]

[8] Apparently it is quite common practice in the Netherlands for convicted criminals to pay someone else to report to prison and be incarcerated in their name. After a couple of weeks incarceration, the 'fake' criminal reports the confused identities and is released. The real criminal has by then disappeared.

[9] Strictly speaking financial identity theft/fraud is a species of criminal identity theft/fraud, as wrongful financial gain is a crime.

22.4.3 Means

Identity fraud may be committed with existing external identities and with newly created identities, as indicated by the fourth subcategory of identity switching, identity creation. Such new identities do not refer to a real person. In general, identity fraud with existing external identities of real persons will be more lucrative, as those identities are already associated with certain (financial) rights and tend to be more credible given their existing history (Koops and Leenes 2006, p. 4). Because new identities do not have any associated (financial) rights yet, they do no lend themselves well for financial identity fraud. Their primary use would be in attracting debt, and not being confronted with the repayment obligations. For criminal identity fraud they may be more useful, as the primary aim is to avoid punishment. A final remark on the difference between existing and new identities is that identity theft may only be committed with the former—in order to steal an identity it must first exist.

22.4.4 Definitions

The above leads to the following definitions. The starting point for these definitions is that the process of identification is inherently flawed, and that errors in the linking of external identities to persons may occur by accident or be intentionally forced. The latter category results in a switched identity.

> An 'identity switch' occurs when someone assumes another external identity—either the existing external identity of a real person or a newly created external identity

Identity switches can be divided into four sub categories. Depending on the circumstances of the case and the applicable jurisdiction, the switch may be wrongful and/or unlawful. If an identity switch is wrongful or unlawful, it is identity fraud.

> 'Identity fraud' is a wrongful or unlawful identity switch

The aim of identity fraud may either be financial gain, financial identity fraud, or the avoidance of punishment, criminal identity fraud. Identity fraud may be committed with both external identities that refer to real persons or with newly created identities that do not refer to a real person. In case the external identity of a real person is used without his consent, the identity fraud constitutes identity theft

> 'Identity theft' is the wrongful assumption of an external identity of another person, without that persons consent.

22.5 Illegality Under Dutch Law

In the United States identity theft and fraud are illegal, if they are instrumental in another crime.

United States Identity Theft and Assumption Deterrence Act[10]:

> '[Punishable is s/he who] knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation Federal law, or that constitutes a felony under any applicable State or local law.'

Unlike the United States, the Netherlands does not have any legislation specifically targeted at identity theft and fraud.[11] That is not to say that the act of committing identity theft and fraud may not be illegal under existing, more general, criminal law. As the name suggests, the traditional crimes most closely related to identity theft and fraud are:

(1) Fraud (forgery and deceit), and
(2) Theft.

The legal definitions of these crimes do however, not provide a perfect fit to various different forms of identity fraud and theft.

22.5.1 Criminal Law—Fraud

The term fraud is used to refer to many different crimes and offenses that in their core have to do with making untrue representations. As identity theft and fraud are an untrue representation of identity, the parallels seem obvious. Dutch criminal law however, does not allow for the application of criminal law on the basis of analogy. An act is only punishable if it matches an existing penalty provision, not because it resembles a certain crime. The provisions of the most fitting traditional crimes are too restrictive to cover all instances of identity theft and fraud. Forgery ('valsheid in geschrifte'—Art. 225, Dutch Criminal Code) only relates to forged documents, and therefore does not apply to identity theft and fraud committed with true (but stolen) identifiers. Various forms of deceit ('opgave onware gegevens en oplichting'—Arts. 227a and 326, Dutch Criminal Code) require that the intent of the crime is financial gain; ruling out their applicability to criminal identity theft and fraud.

---

[10] United States Identity Theft and Assumption Deterrence Act, United States Code, title 18, s. 1028(a)(7).

[11] Currently, a new bill regarding identity fraud in criminal proceeding is pending in the Dutch Senate ('Eerste Kamer') ('Wet identiteitsvaststelling verdachten,veroordeelden en getuigen', Kamerstukken I/II, 31 436). This bill focuses on the prevention of identity fraud in criminal legal proceedings. The bill is aimed at providing a more robust identification process. It however does not introduce penalty provision for identity theft that occurs despite these new attempts at prevention.

22.5.2 Criminal Law—Theft

The general consensus is that identity cannot be stolen in the sense as defined under Dutch criminal law (De Vries et al. 2007, p. 219). Theft is taking away a good that belongs to someone else. To be susceptible to theft, something must first qualify as 'a good.' Whether or not identity can be stolen in a legal sense therefore depends on the definition of identity, and whether that definition fits the requirements of 'good.'

The legal debate on the definition of 'good' for the purposes of theft has a long history. In 1921 the theft of electricity was ruled possible,[12] while in 1996 the possibility to steal computer data was denied.[13] From those cases the following criteria for a 'stealable' good can be derived:

- Autonomous existence—the object must exist in its own right
- Transferable—the object must be transferable
- Controllable—the object must lend itself to human control
- Economic value—the object must represent a certain economic value
- Singularity—if the thief takes control of the object, the rightful owner must at the same time lose control

Electricity conforms to all five criteria, and can therefore be stolen. Computer data fail to meet the fifth criterion as they can be copied. If an illegal copy is made, the rightful owner does not lose control over his own copy; that only happens if the original copy is actively destroyed.

Most authors deny the possibility of theft of identity, because they define identity as information. Under Dutch law it is generally accepted that information cannot be stolen because it lacks singularity.[14] Under my definition of external identity, identity is not mere information but rather the collection of administrated acts that describe a person. Unlike normal information, that collection does posses singularity. If an identity thief takes control of the external identity the rightful 'owner' loses control. There is only one copy of external identity, and if a thief uses it his actions will be recorded in the external identity of his victim; taking away the control the victim once had over his own identity.

The mere fact that external identity possesses singularity may not be sufficient ground to assume that it can be the subject of theft. On the other hand, the observation that external identity is stored as information should not be a reason to deny the possibility of theft of identity. After all, as shown above external identity exhibits the traits traditionally ascribed to goods that be can be stolen.

Classifying identity as a good that can be stolen is controversial and requires some remarks.

---

[12] Hoge Raad (Supreme Court) 23 May 1921, NJ 1921/564.

[13] Hoge Raad (Supreme Court) 3 December 1996, NJ 1997/574.

[14] See among others De Vries et al. 2007, p. 219, and Prins and van der Meulen 2006, p. 11.

First, even if external identity theft would be susceptible to theft, that would not necessarily mean that identity theft would be punishable as ordinary theft. Theft requires the intent to take possession, not just to use the good. The intent of an identity thief will very rarely be the actual possession of the external identity he has targeted. Rather he wishes to use the identity for financial gain or the avoidance of punishment.

Second, and more important, acknowledging the theft of identity would mean widening the scope of the 'theft' beyond what the usually rather restrictive interpretation of criminal law should probably allow.

22.6 A Recent Case of Identity Theft

One of the problems with identity theft is that the perpetrator is hard to catch; if successful, the criminal managed to assume the identity of his victim. His own identity remains a mystery. In most cases of identity theft, multiple parties become the victim: the person whose identity was taken over and the person who was tricked into believing that he was dealing with that first victim. Both will generally be of the opinion that they should not suffer the consequences of the identity theft, face the problem that the person responsible is not to be found. The result is that in most cases of identity theft the aftermath is a battle for compensation between victims.

The case of Ron Kowsoleea is a good illustration.

On 21 October 2008 the national ombudsman published his report on the Dutch Surinam Ron Kowsoleea.[15] According to the report, Kowsoleea has been the victim of identity theft for the last 15 years. Since 1994 the hard drug criminal C. has been passing himself of as Kowsoleea. The police registers crimes perpetrated by C. in Kowsoleea's criminal records. C's identity theft makes two victims: Kowsoleea whose identity is abused and the police that is being deceived.

The information in the police registers has on multiple occasions led to Kowsoleea being arrested, detained, and treated as a hard criminal and undesirable alien. Arrest at Schiphol airport and a raid of his home by 35 armed policemen are the result. Kowsoleea gets convicted by default of appearance for crimes committed by C.[16]

The duration and extent of these effects is remarkable because Kowsoleea already notified the police in 1994 that C was assuming his identity. The police

[15] Nationale Ombudsman 2008, rapportnummer 2008/232, 21 October 2008. The report was later revised to make some factual changes, but the conclusions remained unchanged.

[16] Ibid., paragraph. 28, p. 14. The convictions by default of appearance appear to be the result of the policy of the police to hand out the subpoena directly to the suspect while he is held at the police station. Subsequently the subpoena is no longer served at the home address of the suspect. If the suspect is incorrectly identified at the police office, the person mentioned in the subpoena is not aware that a *subpoena* was served on him.

report recorded that the crimes and offenses were perpetrated by C, not by Kowsoleea. Although the police from that moment on was aware, or should have been aware, that Kowsoleea was the victim of identity theft, they kept treating him as a criminal for the next 15 years. The various police services involved appeared unable to properly record that not Kowsoleea but C. was the criminal. On the basis of that incorrect registration—external identity—they kept treating Kowsoleea as a criminal.

The ombudsman calls the case Kowsoleea, the most Kafka-like case he has ever handled. In his opinion the State's treatment of Kowsoleea was unjust, and warrants an excuse and compensation.

Empowered by the positive verdict of the ombudsman, Kowsoleea summons the State in court.[17] In summary proceedings he petitions for an advance in compensation. The incorrect registrations and the treatment by the police would have been a breach of privacy and a defamation of character. Kowsoleea ask for an advance of € 100,000 in nonmaterial damages. On behalf of his company S.B.V. Kowsoleea also demands an advance of € 300,000 in material damages. The reasoning seems to be that Kowsoleea's bad reputation caused by the police reflects on his company, and has resulted in the company missing out on several important contracts.[18]

The verdict was unpleasant for both Kowsoleea and his company. Their requests for (an advance of) compensation were denied.

That is not surprising. In summary proceedings, the judge is cautious in rewarding monetary claims. Summary proceedings provide neither the space and nor the time to investigate a case in detail. An advance is therefore generally only awarded if it seems likely that compensation will indeed be awarded in proceedings on the merits. In this case that was hard to predict. Identity theft is a new phenomenon. There is hardly any case law. Especially not regarding cases between two victims.

Aside from the problems associated with the type of proceedings, the judge identifies two problems that are of bigger concern.

Every police district has legal personality and is responsible for it's own records and administration. That means that Kowsoleea should not have summoned the State, but rather each separate police district. That is an administrative nightmare. In many cases it will even be impossible, because a member of the public is not aware of all the administrations that hold his personal information.

---

[17] Rechtbank (District court) The Hague 2 March 2009, LJN BH4957.

[18] The case brought by Kowsoleea against the Dutch State was based on civil law, rather than administrative law as is usually the case in proceedings against the State. The claim was based on governmental tort ('onrechtmatige overheidsdaad'). A governmental tort has the same legal requirements as a general tort, but the threshold for establishing wrongful behavior on the part of the State is higher than for a normal (legal) person, as the State has broad powers and authority to justify its actions. The reasoning behind the verdict in the *Kowsoleea* case, being based in civil law, would in principle also apply to cases not involving the State.

The Dutch Border Police that regularly arrested Kowsoleea on Schiphol also escaped unharmed. The Dutch Border Police based its actions on information available in the records of the police. Because it had no influence over the information in those records, the judge is of the opinion that the Dutch Border Police cannot be held accountable for the result of that faulty information.[19]

That in itself is worrying. A member of the public is to turn to the administrators of the administrations that hold incorrect personal information about him. Those administrations are linked, so faulty information in one administration will soon spread to others. It is hard, or impossible, to find out all the administrations that hold the incorrect information. A member of the public will not be in contact with the administrators. Only the users of the information will be apparent to him; the police, the government, the banks, and other private institutions. But those users apparently cannot be held accountable for actions based on incorrect information they do not control.

22.7 Conclusions

Identity has evolved from an internal affair to an externalized matter. External identity is becoming more and more important in our daily lives and interaction with the government, companies and other persons. External identity is susceptible to fraud, and in my opinion: theft. Identity theft and fraud are not only possible, they are also lucrative. As the importance and use of external identities increases, so will the interest of criminals in exploiting it.

Key in understanding and countering identity theft and fraud is an understanding of the concept of (external) identity and the process of identification. With this understanding comes the realization that external identities are not a perfect representation of true (internal) identity and that identification processes are not flawless.

It is therefore na to think that identity fraud and theft can be prevented or eradicated. It would be more effective to focus on preventing and mitigating the damage that results.

This chapter contains two real life examples of Identity theft: debit card fraud and Ron Kowsoleea's case. There is a striking similarity between those cases: in both cases the system was trusted more than the other victim. The bank believed its debit cards could not be copied, and thus concluded that its customers lied. The police believed that Kowsoleea was a criminal because the computer said so.

In addressing identity fraud and theft two separate approaches need attention. On the one hand awareness of the existence of identity fraud and theft is required. The parties involved need to take responsibility and acknowledge that their systems may be at fault. Banks have accepted that debit card fraud exists, and

[19] Rechtbank (District Court) The Hague 2 March 2009, LJN BH4957, consideration 3.6.

reimburse victims (unless the client was clearly to blame). The government so far does not seem to have done the same, given its reluctance to compensate Kowsoleea. Where parties do not take their own responsibility, civil courts should adjudge it. If the *Kowsoleea* case is any indication, the future in this respect may, however, be bleak.

The second approach is through legislation. It is hard to combat identity theft and fraud through prosecution, as the successful perpetrator remains nameless. However, if specific legislation regarding identity theft and fraud is drafted, it should focus on the core aspect of identity theft and fraud: the assumption of identity. Legislation merely focused on the wrongful use of identification means, or on the intent of that use, cannot cover the entire problem—and may become outdated as new means and purposes are bound to present themselves.

References

Clarke RA (1994) Human identification theory in information systems: management challenges and public policy issues. Information Technology & People 4

Foucalt M (1991) Governmentality. In: Burchell G (ed) The foucault effect. University of Chicago Press, Chicago

Grijpink JHAM (2005) Onze informatiesamenleving in wording. Privacy & Informatie 3

Koops BJ, Leenes R (2006) ID theft, ID fraud and/or ID related crime. definitions matter. datenschutz und datensicherheit 9

Kuiper I (2004) Pinpasfraude. Trouw, 2 December

Locke J (1786) An essay concerning human understanding, 19th edn. Dublin (digital reproduction: Thomson Gale, 2003)

LoPucki LM (2001) Human identification theory and the identity theft problem. Tex Law Rev 2001-1:89–135

Marbus R (2009) Identiteitsmanagement in Nederland. de stand van zaken. ECP-EPN, April 2009

Nationale Ombudsman (2008) rapportnummer 2008/232, 21 oktober 2008

O'Harrow R (2005) No place to hide. Free Press, New York

Poster M (2007) The secret self—the case of identity theft. Cult Stud 21:118–140

Prins JEJ (2007) Een recht op identiteit. Nederlands Juristenblad 14

Prins JEJ, Meulen NS van der (2006) Identiteitsdiefstal: lessen uit het buitenland. Jusitit Verkenningen 7

Rost M, Meints M (2005) Authentisierung in sozial systemen. Identity theft strukturell betrachtet. Datenschutz und Datensicherheit 4

Solove DJ (2004) The legal construction of identity theft, symposium: digital cops in a virtual environment. Yale Law School

van der Meulen NS (2006) Achter de schermen: de ervaringen van slachtoffers van identiteitsroof. Justitiele Verkenningen 7

van der Meulen NS (2009) Identiteitsfraude: de eerste stap, nu nog de rest. Computerrecht 38

van Schijndel P (2009) Identiteitsdiefstal. Jongbloed Juridische Uitgevers, Den Haag

Vries URMTH de et al (2007) Identiteitsfraude: een afbakening. WODC

Part VII
Technological Dimensions

Chapter 23
Biometrics and Smart Cards in Identity Management

Bart Jacobs and Erik Poll

Abbreviations

AA	Active authentication
BAC	Basic access control
EAC	Extended access control
EMV	Europay, mastercard and visa
EPC	Electronic product codes
ICAO	International civil aviation organization
MRZ	Machine-readable zone
PIV	Personal identity verification
RFID	Radio frequency identification
SSCD	Secure-signature-creation device
UID	User iDentifier

Contribution received in 2010.

B. Jacobs (✉) · E. Poll
Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands
e-mail: bart@cs.ru.nl

E. Poll
e-mail: erikpoll@cs.ru.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_23,

Contents

23.1 Introduction 420
23.2 The Smart Card Landscape 420
23.2.1 Smart Cards and e-Government 421
23.3 Biometrics 422
23.3.1 Performance and Quality 423
23.3.2 Performance of Face and Fingerprint Recognition 424
23.4 Smart Card and RFID Technology 425
23.4.1 Smart Cards 425
23.4.2 RFID 427
23.5 e-Passports 428
23.5.1 Accessing the Passport Chip 430
23.5.2 Drawbacks of the ICAO Standards 430
23.5.3 Tracking 431
23.5.4 Digitally Signed Passport Data 432
23.5.5 Function Creep 432
23.5.6 Lessons Learnt 433
23.6 Privacy Issues in Using Biometrics and Smart Cards 434
23.6.1 Privacy Implications of Biometrics 435
23.6.2 Use of Smart Cards 436
References 437

23.1 Introduction

The introduction of the electronic passport by governments around the world marks a major step in the use of biometrics. In fact, the electronic passport, or e-passport for short, combines the use of three important technologies for identification: biometrics, smart cards and radio frequency identification (RFID). Smart cards—increasingly often RFID-enabled—are already commonplace in our everyday lives, and the use of biometrics is expected to grow significantly. Apart from being a potential user of these technologies for e-government services, the government also plays an important role as facilitator and regulator of these technologies.

This chapter discusses the technologies of biometrics and (RFID-enabled) smart cards and their use in electronic passports, and reflects on the introduction of e-passports, and the surrounding issues regarding security and the shift in the balance of power between citizen and government. It concludes with a critical review from the privacy perspective.

23.2 The Smart Card Landscape

Smart cards are the leading technology for authenticating users of computer systems whenever something more secure than passwords is needed. The most prominent applications of smart cards are bank or credit cards, and SIM cards in

mobile phones. Digital pay TV systems also use smart cards to control access to transmissions. Many companies (and indeed governments) issue smart cards to their employees to log-on to computers, or access the computer network and on-line services. Smart cards, usually contactless ones, are widely used for physical access control to buildings. Contactless smart cards are also widely used for public transport systems, for instance as the Oyster card in London or the OV-chipkaart throughout the Netherlands.

Apart from serving as authentication token, another important application of smart cards is for digital signatures. Qualified electronic signatures, the strongest form of digital signature under European legislation (EC 1999; CEN 2004), have to be created by a so-called secure-signature-creation device (SSCD). This SSCD is a trustworthy device that stores the sensitive data (cryptographic keys), needed to create digital signatures and performs the computation of digital signatures. Currently, a smart card is the obvious—in fact, essentially the only—choice for an SSCD.

Finally, apart from serving as authentication tokens or SSCDs, smart cards can also be used as secure carriers of information, or data safes. An example is the German 'Gesundheitskarte' that besides identity information contains essentials from the card holder's medical record.

23.2.1 Smart Cards and e-Government

Governments have followed suit in issuing smart cards as authentication tokens to their employees, to selected professional groups, or to all citizens. For example, the US government issues (PIV personal identity verification) smart cards to all government personnel to control physical access to buildings and access to computers and information services; the Dutch government issues smart cards to all its employees (the 'Rijkspas') and to all health-care professionals (the 'UZI pas,' for accessing electronic medical records); the French government issues smart cards to all residents (the 'Carte Vitale') to automate administration in the public health service.

Apart from using smart cards for its own digital services, a question is whether the government should not provide a digital identity to all citizens with a smart card, as associated authentication token for general use. Many countries already issue smart cards to citizens as national electronic ID cards, or eID cards. For an overview of national identity card schemes in the EU and a comparison of their privacy features see ENISA (2009).

There are four main purposes for an eID card:

1. It may be used as an authentication token in the physical world, i.e., used for the same purpose as ID cards, driving licenses or passports have been used for in the past, but with the added functionality that it can be read electronically.
2. It may be used to create digital signatures, serving as a Secure Signature.

3. CreationDevice (SSCD) for qualified electronic signatures.
4. It may be used as an authentication token in cyberspace.
5. It may be used for data encryption and decryption, for instance to enable confidential email exchange.

The third use is what is often called eID, in the narrow sense of the term. The e-passport, discussed in Sect. 23.5, only serves the first purpose—more specifically, proving your identity at border control. Some e-passports can create digital signatures, which allows authentication over the Internet, as discussed in Sect. 23.5, but this is completely unintentional.

23.3 Biometrics

Biometrics refers to the use of physical characteristics or deeply ingrained behavior or skills to identify a person. Physical characteristics that can be used include facial features, fingerprints, iris, voice, DNA, and the shape of hands or even ears. The behavior or skill commonly used for biometric identification is the handwritten signature, but there are more exotic possibilities such as someone's gait, or the rhythm in which someone types on a keyboard. Different types of biometrics have important differences in accuracy, how easy they are to fake, which population groups they discriminate against, how much information they reveal about us, and how sensitive this information is. For instance, your DNA may reveal health risks of interest to insurance companies.

Fingerprints and DNA are different from most other biometrics in that people unintentionally leave copies of their fingerprints and samples of their DNA wherever they go. With the increased use of surveillance cameras, we also leave our facial image and gait in many places. This is what enables such biometrics to be used in law enforcement. It also makes fingerprint information more valuable to the owner, and to potential attackers, as fake fingerprints could be planted at a crime scene.

The big promise of biometrics is, as a more secure and convenient alternative to using passwords to identify users of computer systems. The use of passwords is notoriously insecure and inconvenient. People choose passwords that are easy to guess, reveal passwords to attackers in phishing or social engineering attacks, share them with colleagues, or use the same password at many different places. Biometrics are often seen as addressing these concerns, but they share some of the same problems: you use the biometric information everywhere, you cannot change it, and once compromised there is no alternative: you cannot change your iris or DNA. These issues will be discussed further in Sect. 23.6.

A biometric system works in several steps: its sensors capture a presented biometric, it then processes this input signal to extract features from it, it compares these features to previously recorded and stored biometric information, and finally decides if there is a match or not. Ideally, one does not store the raw biometric information, say an image of the fingerprint, but a template with some information

about features extracted from this raw data. In the case of a fingerprint, this could be information about the so-called minutiae, the bifurcations, and endpoints of ridges in fingerprints, which most fingerprint recognition systems use. Storing such templates goes some way towards protecting the information, and preventing abuse—assuming that fingerprints cannot be reconstructed from the templates.

Biometrics can be used for verification or identification. In verification, a person is matched with one particular stored biometric, for instance the fingerprint on his e-passport, to check that someone has a certain claimed identity. In identification, a person is matched with a large collection of stored biometrics, for example to see if his name occurs in a database of known criminals, or has not already applied for a passport under a different name. When it comes to the quality of biometric systems, discussed below, identification is a lot more error-prone than verification, simply because it involves many one-to-one matches so that errors accumulate.

23.3.1 Performance and Quality

Biometric systems are not perfect. When trying to match a stored biometric with one freshly obtained, there is always the chance of false matches and false non-matches. A false match occurs when the system reports a match when in fact the stored biometric comes from someone else. A false non-match occurs when the system reports that the two do not match, even though both are from the same person. False matches are often called false accepts, and false non-matches are false rejects, but beware that this terminology can be confusing: if a database of biometrics is used to check that known terrorists do not enter the country, then a false non-match leads to a false accept (into the country), not a false reject.

Exact rates of false accepts and rejects depend on the type of biometric used—some are considerably better than others—and the particulars of the system. When a biometric system is used for identification, as opposed to verification, the false match rate will increase linearly with the size of the database: as the database with stored biometrics increases in size, the false match rate will increase and may become too large for the system to be useful. Also, within certain boundaries, there is a trade-off between the false match and non-match rates: by tuning up the precision required for a match, the false non-match rate of a system can be decreased at the expense of a higher false match rate. A lot of research has to go into the optimal tuning of a system to get a good balance. Here, it very much depends on the purpose of the system whether one would prefer a higher false reject rate or a higher false accept rate. An important issue is also who controls the tuning. Entry guards hate false non-matches because of the hassle—angry customers—these cause. Hence, they will be inclined to minimize false non-matches, leading possibly to a greater risk of false matches—including the scenario of a terrorist entering the building.

Another important quality measure of biometric systems is the failure to enroll, the percentage of users for whom it is not possible to obtain the required biometric

information. Here, biometric systems may exclude or discriminate against certain population groups. For example, for biometric systems using fingerprints, people may be unable to enroll because they miss fingers, or also because they are older (as the quality of fingerprints deteriorates with age), very young, work as bricklayers, or suffer from arthritis (which hampers the taking of fingerprints). Also, some forms of medication affect the quality of fingerprints.

Another quality measure is how easy it is to fool a biometric system by spoofing some fake input to the system, e.g., using a rubber copy of a fingerprint, which any competent DIY-er can make, given a fingerprint image (van der Putte and Keuning 2000). Famously, some fingerprint detectors can be fooled by simply breathing on them, which causes them to recognize the residue of the fingerprint left by the previous user (Thalheim et al. 2002). Systems can try to make this harder, e.g., fingerprint detectors can measure the temperature or heart beat of the presented finger, but this will never be foolproof. This problem gets a lot worse for unsupervised biometric systems.

23.3.2 Performance of Face and Fingerprint Recognition

Prior to the introduction of the e-passport, a large trial was conducted in the Netherlands in which nearly 15,000 people were issued with test passports containing facial images and fingerprints (MBKZ 2005). The aim was to test the enrollment procedures and the quality of biometric systems.

The trial also included automatic face recognition. In 2.2% of the cases the facial image could not be verified when people collected their passports. Here people wearing glasses had a higher chance of a false reject. Note that people were matched with images taken only a week earlier, when they applied for a passport; over a longer period, one can expect the false non-match rate to increase significantly, as people grow beards, have haircuts, or simply age.

In the trial two fingerprints were taken. In the enrollment phase, fingerprints could not be recorded in 3.2% of the cases: in 1.9% of the cases it was impossible to record any fingerprints, in 1.3% it was only possible to record one. In the verification phase, in 4.3% of the cases, one finger could not be verified; and in 2.9% of the cases, neither finger could be verified.

These percentages are large enough to have a big impact. For example, in the Netherlands it has been decided that when someone collects his e-passport at city hall, it will not be checked if his fingerprints match those stored on the passport—collected upon application for the passport the weeks before—because the expected number of false non-matches would cause too much hassle at the counter. How such expected false non-matches will be handled at border controls is unclear at this stage. More generally, it is clear that automated passport controls using biometric systems will not be possible without extensive fallback procedures to deal with substantial numbers of false rejects.

To get an impression of false match rates when fingerprints are used for verification, as opposed to identification, with large sets of data: the US-VISIT system, which checks fingerprints of visa applicants against a database with information of 6 million people, was reported to have a false match rate of 0.31% (Wilson et al. 2004). Here false matches cause hassle for innocent travelers, whereas false non-matches let unwanted people into the country. By changing operational parameters of the system, the false match rate could be reduced to 0.08%, at the expense of increasing the false non-match rate from 4 to 5%.

Getting reliable-independent data on the accuracy of biometrics in such large scale—essentially global in the case of e-passports—applications is important for judging the technology.

23.4 Smart Card and RFID Technology

This section discusses characteristics of smart cards, and RFID-enabled contactless smart cards, and the security they can offer, when used in electronic passports or other applications.

23.4.1 Smart Cards

A smart card is a tiny computer, contained on a single chip. Traditionally these chips were embedded in a piece of plastic the size of a credit card, but over the years variations in form and appearance have been introduced. Apart from its small size, the prime characteristic of a smart card is that it provides security: it offers protection against unauthorized reading or modification of data on the card. The software on the card can enforce restrictions on data being read or modified, for instance allowing certain operations only after a user has been authenticated by means of a PIN, or never letting confidential information, for instance cryptographic keys, to be read from the outside. A smart card can provide protection to the information on the card even against someone who has physical access to the card. This means an organization can issue cards to users even if it does not trust these users, or does not trust them not to loose their cards.

All this makes smart cards radically different from more old-fashioned magnetic stripe cards, which offer no protection whatsoever to the data stored on the magnetic stripe. Magnetic stripe cards are easy to clone, which has led to skimming attacks, where criminals copy magnetic stripes and spy on people entering their PIN, to then use cloned cards to withdraw cash anywhere in the world. The huge rise in skimming attacks has led to many banks switching over to smart cards, typically so-called EMV cards implementing the standard developed by Europay, Mastercard, and Visa. Compliance with EMV is also promoted by the European Payments Council, as part of the implementation of the Single Euro Payments Area.

Replacing magnetic-stripe cards and handwritten signatures by smart cards and PINs might not be a security advantage for all parties involved, as the move may be accompanied with a shift in liability in case of fraud or disputes. In the UK, the introduction of EMV cards has lead to some public debate (Anderson et al. 2006), as customers are by default responsible for fraud committed with their smart card and PINs, whereas they are less likely to be held accountable for fraud committed with old-fashioned credit cards and handwritten signatures.

Smart Cards are the natural choice for secure storage of biometric information. The card can protect the information, it cannot easily be cloned, and even if a card is lost or stolen, the protection it provides remains in place. In the case of an e-passport implementing Extended Access Control, as discussed later, this means the biometric information cannot easily be read from a stolen passport. Also, if people are allowed to carry their own smart card with their biometric information, this sensitive information is then under their own physical control.

Although card holders carry 'their own' smart card with them, and control physical access to the cards, the card issuer usually retains legal ownership of the card and remains in complete control over the software and data on the card. In other words, the issuer keeps complete 'logical' control over the card. So the balance of power is very much in favor of the card issuer rather than the card owner. This does not mean that the card issuer can access any data on the card; cards are (or should be) designed so that private keys and PIN codes on the card are inaccessible to the issuer.

When using biometrics for verification, an ideal solution would be to implement.

The entire biometric system on the smart card, so that the matching of the biometric is done on the smart card. The stored biometric information then never has to leave the smart card. Prototypes of such cards have been made, even with on-card sensors to take fingerprints. Unfortunately, the processing power needed for this exceeds what is currently available on reasonably priced smart cards. So, typically the smart card only provides the biometric information to an external biometric system that does the job of matching.

The security that smart cards provide is not 100%. Using highly specialized techniques and equipment, it may be possible to read or even modify the data on the smart card in unwanted ways. In other words, smart cards are not tamper-proof, but only tamper-resistant. For instance, close observations of the tiny variations in the power usage of a smart card may reveal cryptographic keys used on the card; shooting a laser beam at the chip may change a few bits of data, even though doing this in a controllable and meaningful way is extremely hard. Apart from such physical attacks, there may be bugs in the software on the card that can be exploited. Fortunately, the software on a smart card is relatively simple, and the chance of such bugs is therefore a lot smaller than, say, for a PC operating system. However, as the software on smart cards grows in complexity, the chances of such software bugs will increase. Continued technological improvements and the ongoing arms race between new attacks and new countermeasures mean that a smart card's security has a limited shelf-life. Cards that are a decade old should not

be considered secure. This is an issue in setting the validity period for say e-passports, which some countries chose to reduce to 5 years.

23.4.1.1 The Terminal Problem

An important and fundamental limitation in the security that smart cards can provide is caused by the absence of a keyboard or a display on the smart card. Because of this, the card holder cannot communicate with his smart card without the help of some other device that does have a keyboard and display. In the case of a SIM card this device is the mobile phone; in the case of your bank card it is an ATM or card reader in a shop. This device has to be trusted to keep communication between the card holder and the smart card, confidential and not to change what is being communicated.

For example, if you type your PIN on some card reader to buy something with your credit card, you have to trust the display for the amount you are paying, and you have to trust the device not to secretly store or reveal your PIN in some way. Using your card in a mafia-operated shop could cause problems. Criminals have gone as far as installing completely bogus but convincing-looking ATMs in efforts to defraud people. Similarly, if you insert a smart card in a PC to digitally sign some document, then a computer virus on your PC could change the document before it is signed, or simply sign something completely different than what is displayed on the screen. This security threat is why some banks provide customers with a smart card reader with a small display and a keyboard for internet banking; using a smart card reader hooked to the PC, and then using the standard keyboard and display would also be possible, but this introduces the risk of PC-borne attacks on internet banking.

More generally, securing the link between a computer system and the human user is a big problem. Paradoxically, we know how to secure the connection between computers (including smart cards) hundred of miles apart, even if these communicate over completely untrusted communication channels such as the internet. Securing the last two feet from the computer to the human user is much harder. Biometrics could be used here to authenticate the human user to the system, but not the other way around! However, remote use of biometrics, say over the internet, is fraught with difficulties: the remote biometric system can be physically tampered with, and fake inputs can be spoofed, all without risk of detection.

23.4.2 RFID

Traditional smart card have metal contacts which are used for the electronic communication. Increasingly, however, smart cards are contactless. The chip is then equipped with an antenna for communication using radio waves. This technology is called (RFID Radio Frequency IDentification). Contactless smart

cards can be hard to recognize, as the chip and antenna can be embedded inside plastic or paper, as is the case in the e-passport, and cannot be seen from the outside.

RFID devices, also called RFID tags or transponders, come in different shapes and sizes. More importantly, different types of RFID devices vary considerably in the distance at which they can be activated, and in the computing power they have.

The RFID cards in e-passports are so-called proximity cards, which implement ISO 14443 standard. Proximity cards are widely used for access control to buildings and public transport. The typical operating distance for proximity cards is a few centimeters, but cards can operate at greater distances, using a larger and more powerful antenna in the reader, which raises obvious privacy concerns. Here it is important to distinguish between attacks where someone tries to activate a tag without the owner knowing and attacks where someone only wants to eavesdrop on the communication when the tag is used with the owner's consent at a legitimate reader: the maximum distances for activation and for eavesdropping are different. For ISO 14443 proximity cards, remote activation has only been demonstrated at 27 cm (Hancke 2006) and theoretical predictions of what might be possible, do not exceed 60 cm (Kfir and Wool 2005; TI 2003). Eavesdropping is possible at larger ranges: theoretically it is possible at up to 4 m, practically it has been demonstrated at 2.5 m (BSI 2008). Note that the experiments above were done under carefully controlled circumstances, and will be hard to achieve in practice.

The simplest RFID tags do not have any computing power whatsoever, unlike the e-passport. All these tags can do is broadcast their unique serial number when activated, without any form of encryption. Such devices are commonly injected in domestic pets for identification and are set to replace optical bar codes in many application, as so-called Electronic Product Codes (EPCs).

Surprisingly, given the obvious risks to privacy, EPC tags are used in some identification documents: in the USA, they are used in the Washington State 'Enhanced' Driving Licenses and in the Passport Card, a credit-card sized travel document for travel to Canada and Mexico. These RFID tags are very different from the proximity cards used in e-passports: they have a much greater range, and have been successfully activated from distances of 10 m or more (Koscher et al. 2009), as opposed to 27 cm. Moreover, as these tags only broadcast some serial number, they can easily be cloned or spoofed, and allow easy tracking.

23.5 e-Passports

Electronic passports—e-passports for short, also called biometric passports—have a contactless smart card chip embedded in one of the passport pages.[1] E-passports were introduced in the wake of the 9/11 attacks, when the United States

[1] Prior to the introduction of smart cards in passports, passports were already machine readable in the sense that the bottom of the main passport page, the so-called machine readable zone (MRZ), can be automatically read using Optical Character Recognition (OCR) technology.

government announced it would require passports to have embedded chips with biometric information in order to travel to the US under the Visa Waiver Program. However, in Europe discussion about of e-passports and use of biometrics was already underway earlier. (By the way, all 9/11 hijackers carried valid passports, and the requirement to carry valid electronic passports would not have posed any additional obstacle in carrying out the attacks.) The International Civil Aviation Organization (ICAO), an agency of the United Nations, defined the international standard for the e-passports. The ICAO specifications still offers the freedom of various options, but guarantee basic interoperability of passports and inspection systems. Apart from facial images, the ICAO standards currently support the use of fingerprint and iris information as biometrics.

As an additional security measure, embedding chips in passports makes them harder to forge. However, as modern passports are reputedly hard to forge already, this does not seem to have been the main motivation for e-passports. Given that passports are hard to forge, much of the fraud with passports is through so-called look-alike fraud, where someone uses a real, but stolen or bought passport belonging to someone else who looks sufficiently similar. The facial images stored on the chip, which provide a higher resolution than a classic passport photo, could make look-alike fraud harder, as would any additional biometric information stored on an e-passport. The information could also be used to make it harder to obtain a passport in someone else name, but only if the issuing organization has records of previous applications. It is unknown how often such double applications occur.

The ICAO specifications (ICAO 2007) provide three security measures for the e-passports: passive authentication (PA), active authentication (AA), and basic access control (BAC).

On top of this, the EU has adopted Extended Access Control (EAC) (BSI 2006) as an additional, stronger security mechanism for the fingerprint information in the second generation of e-passports, as this is considered more sensitive biometric information.

Both passive authentication and active authentication make it harder to make fake passports or tamper with a real one. Passive authentication authenticates the data on the e-passport, by means of a digital signature over this data. This signature proves the data on the passport is authentic and has not been altered in any way. To verify the digital signature one needs the public key certificate of the issuing country. Passport inspection systems have to be supplied with public key certificates of individual countries to be able to verify that the e-passport data carries the correct digital signature. Active Authentication, authenticates the chip in the passport, by means of a challenge-response protocol, where the chip effectively digitally signs some random challenge sent to the chip. The chip carries its own public key certificate, signed by the issuing country, to provide that this signature is authentic. Passive Authentication is mandatory in the ICAO specifications, Active Authentication is optional. Although the e-passport is not intended for any on-line use, active authentication can be used for on-line authentication over the internet (van Dijk and Oostdijk 2009).

23.5.1 Accessing the Passport Chip

Basic access control (BAC) prevents access to the information on the passport chip without the user's consent. Because passport chips are contactless, an attacker could try to eavesdrop on the wireless communication between the e-passport and a legitimate passport terminal, say at a border control at the airport. An attacker could also secretly activate the passport chip while it is in someone's bag or pocket and communicate with it by holding a reader close to it. These dangers would not exist with a contact chip, where the user must visibly give consent to anyone accessing it, by inserting it in a reader. The main motivation for making the chip contactless has been convenience: contactless smart cards allow higher data rates, are less likely to fail because of dirt or wear and tear on the contacts, and are simply more convenient to use.

Some countries, including the USA, have introduced metallic shielding in the passport cover. Thin foil in the cover acts as a Faraday cage, making it impossible to activate the chip when the passport is closed. Note that this does not protect against eavesdropping, as the passport will have to be opened at passport control.

The (optional) mechanism of BAC provides protection against both eavesdropping and remote activation. With BAC, access to the chip is protected by an access code, preventing remote activation, and this access code is also used to encrypt communication between the e-passport and the terminal, preventing eavesdropping. The access code is part of the information that is written in the passport at the bottom of one of the passport pages, on the so-called machine readable zone (MRZ). This information is optically readable, and is for instance used for automated check-in at some airports. The access code consists of the passport number, the date of birth of the passport holder, and the expiry date of the passport. Having the access code written in the passport may seem strange, but the basic idea makes sense: only as you hand someone your passport and thereby give them permission to open and read it, do you give them access to the chip.

23.5.2 Drawbacks of the ICAO Standards

A fundamental weakness of BAC is that, after eavesdropping on communication between e-passports and readers, an attacker can mount a brute force attack trying out all the possible keys. A proper password-based key exchange protocol would be better, and is in fact incorporated in extended access control (EAC). This weakness in BAC is aggravated by the poor randomness of the access codes in the MRZ. At best, the total entropy in the MRZ is only 72 bits (Hoepman et al. 2006), which is less than current recommendations. If countries issue passport numbers in sequence, so that these are predictable and strongly correlated with the expiry date, this can reduce the search space substantially and make a brute force attack quite feasible.

Active authentication prevents the cloning of passport chips by adding what is essentially digital signature functionality to the e-passport. The downside is that, this way passport can be made to sign anything, by invoking the AA functionality, without the passport owner knowing.[2] Although the intention is that the passport inspection system just sends a random number to be signed, a system could sent a specific number with some meaning, for instance a coded string saying 'passport nr 1234567X was at Heathrow airport on May 12, 2010.' The data that the card will sign is only small (8 bytes), but this is enough to code up some meaningful information, say time + GPS data. The chip authentication procedure that is part of EAC completely avoids this possibility, by using a different method for authentication.

Extended access control improves BAC by providing a key exchange protocol that is more resistant to off-line brute force attacks, and improves AA by providing a chip authentication protocol that does not suffer from the signature problem. EAC also adds the possibility for the passport to authenticate the terminal. This allows the e-passport to only release fingerprint or other sensitive biometric information if the terminal can provide a certificate, issued by the government of the country that issued the passport, giving the terminal the right to do so. Each country can decide which other countries have the right to read this data from their passport, and give these individual countries digital certificates allowing them to do this. This means that someone stealing a passport cannot access the sensitive biometrics on the passport chip, without stealing an official passport inspection system from customs, or at least the certificate it contains. Certificates of passport inspection systems will be short-lived, valid only for 6 months, to reduce the impact of them being lost or stolen. All this requires a complex infrastructure to manage certificates. Countries will have to exchange digital certificates by diplomatic mail, and periodically update the certificates in all the passport inspection systems, used throughout the country.

23.5.3 Tracking

BAC and EAC regulate access to the data stored on the passport chip, but do not address the possibility that the chip itself can be remotely recognized. As specified in the ISO 14443 standard, upon activation, an RFID tag broadcasts some arbitrary number, a so-called UID, to begin the communication. On most RFID tags this UID is a fixed arbitrary number; this number can then be used to identify an individual passport. To prevent this, in passports a different, randomly generated number should be used as UID each time the chip is activated. Most countries now use such chips, but at least initially some passports with fixed UIDs have been issued.

Even if passport chips send out random UIDs, so that an individual passport cannot be recognized, passports from different countries are likely to use different

[2] Of course, AA is only possible after BAC.

hardware and software, which are then likely to exhibit some observable differences in behavior. Indeed, it turns out that passports from many countries can be distinguished automatically before BAC takes place (Richter et al. 2008). Only if countries buy e-passports from the same vendor, and use identical hardware and software, can this be ruled out.

23.5.4 Digitally Signed Passport Data

The possibility of tracking people via their e-passport has attracted most attention in discussion of the risks of e-passports, but there are other, less spectacular, consequences.

The information on e-passports is digitally signed to prove its authenticity. A fundamental aspect of a digital signature, as a means of authenticity is that it can be stored and transferred. In the case of the biometric information protected by EAC, it means that if country A gives country B permission to read such biometric data from their citizen's passports, there is nothing to prevent country B from storing this data, with the digital signature, to use at some time later, or to pass on to some other country or party who did not get permission from country A to access the information. Moreover, as the data is digitally signed, anyone who gets the data can still check the signature.

In essence, the passport chip does not just show a photograph and say that this is really the facial image of the passport holder, but it effectively hands over an infinite number of witness-signed copies of the photograph which the reader can (re)use and re-distribute at will. And whereas a photocopy of a passport page does not carry the same authority as the original, a digital copy of an e-passport's digitally signed data does.

More generally, digital signatures make information more valuable to potential users, both legitimate, and illegitimate ones, and make loss or theft of the information more of a concern for the owner. There is a difference between my passport photo showing up on the internet or a digitally signed passport photo—digitally signed by the Dutch government to prove it's really me—ending up on the internet.

From a privacy point of view, a safer alternative to digitally signing the data would be to use a protocol which does establish authenticity of the data, but which does not provide transferable proofs of authenticity (Monnerat et al. 2007). Alternatively, one could authenticate the chip, for instance as is done in EAC, and then rely on authenticity of the chip to ensure that the (unsigned) data it provides, is also authentic.

23.5.5 Function Creep

For the e-passport to work it is only required that someone's biometric data is stored in the chip of their passport, and nowhere else. However, once the

authorities collect the data for the production of e-passports, there is the temptation to also store this information in a database. And once the information is stored, there will be temptation to use it for a growing list of applications, a phenomenon known as function creep. As a case in point, the Dutch government is setting up a central national database, and whereas originally this data was to be collected only to support the process of issuing passports, the scope has been widened to also use it for law enforcement. One may question whether the potential benefits warrant the infringement of privacy and civil liberties, or indeed whether the government should treat all its citizens as potential criminals. One may also question the usefulness of such a national database; if the data is used for verification, e.g., to find a burglar after fingerprints have been found on a crime scene, a large database containing biometric data of huge numbers of law-abiding citizens might not be so useful, given that the chance of false matches increases with the size of the database. Innocent citizens with a similar fingerprint to some serious criminal might experience considerable nuisance. (Note that the false match rates for fingerprint recognition mentioned earlier concern high quality fingerprints taken under controlled circumstances, not partial or smudged fingerprints lifted from a crime scene).

The highly decentral storage of sensitive biometric data on individual passports is much harder for any attacker to abuse on a large scale than a central database, which could be hacked by outsiders, or abused by insiders. An attacker would need physical access to the actual passport to obtain its data and, if the passport implements Extended Access Control, the attacker would also have to steal a valid terminal certificate. In practice this means that only countries which have such terminal certificates can collect large amounts of sensitive biometric data, by harvesting it at border controls.

23.5.6 Lessons Learnt

A serious shortcoming in the e-passport from a privacy perspective is that for fingerprints the raw biometrics—images of the fingerprint—are used. Storing a template does not necessarily rule out the possibility of abuse by someone producing fake input to the sensors of a biometric system, but it would rule out someone abusing the information to fake fingerprints marks.

Looking back at the introduction of e-passports, it is clear that the original ICAO specifications could be substantially improved. As discussed, both BAC and AA were found to have weaknesses. Weaknesses can simply be that security measures can be improved, e.g., BAC provides some security, namely protection against eavesdropping, which could be improved, as is done in EAC. Weaknesses can also be that security is at odds with privacy. For example, AA provides extra security (protection against fake passport chips) at the expense of privacy (the threat of unwittingly putting digital signatures), which is avoided by EAC.

PA provides extra security (protection against fake passport data) comes at the expense of privacy (the leaking of digitally signed data).

Apart from aspects that could be improved in the standards, some individual countries also slipped up with the introduction. Some countries, including the USA and Belgium, did not implement BAC in the first e-passports they produced. Several countries, including the UK and Belgium, issued passports with very little entropy (randomness) in the Machine-Readable Zones. Some countries issued e-passports with RFID chips that had a fixed, unique UID, so that passports can be tracked. Again, a more general lesson here seems to be that some time and reflection, should be taken to avoid such mistakes.

23.6 Privacy Issues in Using Biometrics and Smart Cards

In access control one usually distinguishes three stages:

- Identification: saying who you are, for instance via a login name, bank account number, or social security number.
- Authentication: proving who you are, for instance via a password or a PIN.
- Authorization: establishing what someone is allowed to do.

We shall briefly review to what extent biometrics may be useful in the first two of these stages. Authorization is a separate process that is in principle unrelated to the means of identification and authentication.

Biometrics is definitely useful for identification. A key aspect of any biometrics, irrespective of the type, is that it uniquely identifies a person via certain physical or behavioral characteristics. Of course, the biometrics may be spoofed, just like a login name may not be yours, but remember we are discussing identification, not authentication at this stage. Identification is only the first step towards authentication. Biometrics is useful and easy to use for identification simply because you always carry it along.

Is biometrics also useful for authentication? Proper authentication is important because it may not only give you certain (access) rights, but may also bind you to certain obligations. The latter is often called non-repudiation and implies that you cannot refute or deny certain actions that you have performed, like in signing a letter. Biometrics for authentication is much more problematic. It assumes that:

1. Only you are the source of fresh biometric measurements.
2. Freshness of such measurements can be recognized.
3. You provide input to these fresh measurements voluntarily and consciously.

Only if all three points hold convincingly, biometrics can be used to hold people accountable. But as mentioned in Sect. 23.3, breathing on a fingerprint reader may be enough to reactivate the previous measurement. This undermines all three points.

These three points are highly problematic. A database storing biometric information is a dangerous source of non-fresh measurements. Therefore it is essential that only abstract feature templates are stored so that the original measurement cannot be reconstructed. Ensuring this is beyond the control of the person supplying the fingerprint. Even if only templates are stored, upon each fresh measurement, one runs the risk that the biometric device surreptitiously stores the measurement itself.

This issue becomes more and more urgent with the increasing number of biometric applications and the ensuing risk of interaction and interference. Suppose two stores A and B both use my fingerprints in a payment application, so that I do not need to carry my bank card and remember my PIN, but can simply pay by putting my finger on a biometric reader device. This may offer convenience, but it offers very little security: for instance an employee with access to A's database may spoof my fingerprint at shop B and pay on behalf of me. This shows that fingerprints, or any other form of biometrics, are unsuitable for non-repudiation. In fact, in a few years time all the countries that I travel to will store my fingerprint, making it effectively useless for any security-sensitive form of authentication.

Certain high security facilities do use biometrics for access control. But they typically do not use it as their only form of access control and require some form of human supervision. Moreover, they use a relatively non-standard form, like hand-palm or iris recognition, which is not used in many other places and are (therefore) more difficult to spoof. But clearly, if such forms become more widespread, their reliability decreases rapidly.

The conclusion is that biometrics may look convenient, but can essentially only be used for identification. It may be used as input for authentication—requiring an additional, different proof step, just like for a login name—but it should not be used as authentication itself. Being able to tell a social security number is also not a reliable proof of—even though it is sometimes accepted as such.

23.6.1 Privacy Implications of Biometrics

We identify several privacy concerns related to biometrics. First, as already mentioned, biometric measurements may contain much more information than is strictly needed for identification. This is most obvious with DNA, which contain a lot of information about your genetic build up—and of subsequent generations. Much of what is exactly contained in DNA is still poorly understood, but now already certain sensitive health risks may be visible.

Secondly, when improperly stored—as original measurements and not as abstract templates—biometrics may actually increase the risk of identity fraud. When a biometric database becomes compromised, or in the worst case becomes public, for instance via hacking or negligence, the stored measurements may be used for false authentications. This assumes that use of biometrics for authentication will continue, despite its unsuitability.

Thirdly, biometric information may be used for tracing people, either openly, for instance via public security cameras, or covertly. Tracing is primarily based on identification, not on authentication. Such tracing is based on biometric identification and assumes an already established database of measurements for look-up. National databases of fingerprints that several countries (including the Netherlands) are now building may be used for such purposes. They lead to a shift in the balance of power between state and citizens, as with such databases, the state can identify people against their will.

23.6.2 Use of Smart Cards

Are smart cards Big Brother's little helper (as phrased in Brands 2000) or can they empower people? Actually both, but the emphasis in current deployment is more on the former than on the latter. Smart Cards are most often forced upon people together with the obligation to use them on many occasions to authenticate themselves. Via such applications people leave traces and become less anonymous. Moreover, each authentication obligation may involve the transfer of personal information stored on the card, as in the case of e-passports. This traceability may happen in a subtle, unconscious manner, when wireless smart cards use fixed UIDs, that they reveal every time they enter into the magnetic field of a card reader, see Sect. 23.5.

An essential aspect of (informational) privacy is being able to control access to one's own personal information, and keeping such information segmented in different spheres and roles in one's life. Smart Cards may actually be useful for such purposes, because they provide secure storage of a limited amount of data and, more importantly, of personal cryptographic keys. With these keys one can encrypt personal data, so that local, in context storage is no longer essential: as long as I control the keys that are required for decrypting my information I do not care very much where this (encrypted) information actually resides 'in the cloud.'

More advanced modern smart cards have substantial computing power that allows them to perform non-trivial cryptographic operations which can be used for privacy friendly applications. A clear example is provided by anonymous digital cash, as originally proposed by David Chaum (Chaum 1985; Chaum et al. 1988). There is more recent interest in privacy-friendly protocols for attribute-based authorization, like in Brands (2000). Access to many situations is based on possession of proper attributes, like having a valid ticket for entering a bus or a train, or being over 18 for buying alcohol. Such attributes need not involve an identity. But when your entire eID is read electronically at a liquor shop when you only need to show that you're over 18, there is an obvious overkill. It can lead to many forms of unwanted profiling or even to identity fraud. Similarly, with the introduction of smart cards for e-ticketing in public transport a (silent) transition has taken place from attribute-based to identity-based authorization. Research is going on to make modern selective disclosure protocols run on advanced smart cards, see

e.g., Batina et al. (2010) and the references therein, so that upon entering a train or bus, a card can for instance securely demonstrate that it is a valid month card, without revealing its (card or owner) identity.

References

Anderson R, Bond M, Murdoch S (2006) Chip and spin. Comput Secur J 22(4):1–6. http://www.chipsandspin.co.uk

Batina L et al (2010) Developing efficient blinded attribute certificates on smart cards via pairings. In: Gollmann D, Lanet J-L (eds) Smart card research and advanced application conference (CARDIS 2010), number 6035. Lecture notes in computer science. Springer, Berlin, pp 209–222

Brands S (2000) Rethinking public key infrastructures and digital certificates: building in privacy. MIT. Freely available via http://www.credentica.com

BSI (2006) Advanced security mechanisms for machine readable travel documents—extended access control (EAC). Technical report TR-03110. Federal Office for Information Security (BSI)

BSI (2008) Messung de Abstrahleigenschaften von RFID-Systemen (MARS) Specifications. 1: Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation. Technical report. Federal Office for Information Security (BSI)

CEN (2004) Guide on the use of electronic signatures—part 1: legal and technical aspects. http://www.cen.eu

Chaum D (1985) Blind signatures for untraceable payments. In: Chaum D, Rivest RL, Sherman AT (eds) Advances in cryptology: proceedings of crypto'82. Plenum Press, New York, pp 199–203

Chaum D, Fiat A, Naor M (1988) Untraceable electronic cash. In: Goldwasser S (ed) CRYPTO 1988, number 403. Lecture notes in computer science. Springer, Berlin, pp 319–327

EC (1999) Directive 1999/93/EC of the European parliament and of the council of december 1999 on a community framework for electronic signatures

ENISA (2009) Privacy features of European eID card specifications. Technical report, European Network and Information Security Agency (ENISA)

Hancke G (2006) Practical attacks on proximity identification systems. In: IEEE symposium on security and privacy (S and P'06). IEEE, pp 328–333

Hoepman J-H et al (2006) Crossing borders: security and privacy issues of the European e-passport. In: IWSEC 2006: Advances in information and computer security, number 4266. Lecture notes in computer science. Springer, Kyoto, pp 152–167

ICAO (2007) Supplement to Doc 9303, Version 6 (Final). Technical report, ICAO.http://mrtd.icao.int

Kfir Z, Wool A (2005) Picking virtual pockets using relay attacks on contactless smartcard systems. In: First international conference on security and privacy for emerging areas in communications networks (SECURECOMM'05). IEEE

Koscher K et al (2009) EPC RFID Tags in Security applications: passport cards, enhanced drivers licenses, and beyond. In: ACM conference on computer and communications security. ACM, pp 33–42

MBKZ (2005) Evaluatierapport biometrieproef 2b or not 2b. Technical report, ministry of the interior and kingdom relations

Monnerat J, Vaudenay S, Vuagnoux M (2007) About machine-readable travel documents. In: RFID security, pp 15–18

Richter H, Mostowski W, Poll E (2008) Fingerprinting passports. In: NLUUG spring conference on security, pp 21–30

Thalheim L, Krissler J, Ziegler PM (2002) Körperkontrolle—biometrische zugangssicherungen auf die probe gestellt. C't magazin, p 114. English translation, entitled 'body check: biometrics defeated' by RW Smith, available at http://www.extremetech.com/article2/0,2845,13919,00.asp

TI (2003) Radio Frequency identification systems HF antenna design notes. Technical report 11-08-26-003, Texas instruments

van der Putte T, Keuning J (2000) Biometrical fingerprint recognition: don't get your fingers burned. In: Domingo-Ferrer J, Chan D, Watson A (eds) Proceedings of the fourth working conference on smart card research and advanced applications (CARDIS 2000) IFIP Conference Proceedings Vol 180. Kluwer, Bristol, pp 289–306

van Dijk D-J, Oostdijk M (2009) Using the ePassport for online authentication. Technical report TI/RS/2009/002, Telematica Institute

Wilson C, Garris M, Watson C (2004) Matching performance for the US-VISIT IDENT system using flat fingerprints. Technical Report NISTIR 7110. National Institute of Standards and Technology (NIST)

Chapter 24
How Devices Transform Voting

Wolter Pieters

Abbreviation

STV Single Transferrable Vote

Contents

24.1 Introduction 440
24.2 Voting Requirements 440
24.3 e-Voting in the Netherlands 441
24.4 Implicit Requirements 442
24.5 The Theory of Technological Mediation 444
24.6 Technology Mediates Voting 445
24.7 Challenges 446
24.7.1 Voting System 446
24.7.2 Autonomy 447
24.7.3 Secret Ballot/Privacy 448
24.7.4 Verifiability 449
24.7.5 Example: Estonia 450
24.8 Conclusions 451
References 451

Contribution received in 2010.

W. Pieters (✉)
Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands
e-mail: w.pieters@utwente.nl

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_24,

24.1 Introduction

Several European countries have been involved in the implementation of electronic forms of voting in elections. This may include electronic voting machines at polling stations, Internet voting, or both. In the former, the registration and counting of the votes are done electronically, but authentication of the voter and the protection of the secrecy of the ballot still depend on traditional means. In the latter, voting is done remotely from any computer, and the polling station is abolished as protective space.

To allow observation of the elections (Vollan 2005), it is deemed essential that the voting procedure be verifiable. From a technical perspective, the combination of voter anonymity and verifiability is challenging. However, even if a satisfactory technical solution were found, electronic forms of voting challenge the democratic process in other ways. Whereas technology once had the reputation of contributing to explicit goals in an instrumental way, philosophers have now realized that it also changes our experience and existence in ways that had not been intended. Moreover, many requirements of procedures to be automated are implicit, and the automated versions may thereby 'act' differently.

In this contribution, I analyze how electronic voting shapes democratic forms of voting from the perspective of technological mediation. First of all, I introduce the requirements that are generally accepted to apply to the voting process. I then zoom in on the history of electronic voting in the Netherlands, explain how the country finally abolished electronic voting, and recast the problems encountered in terms of implicit requirements. I then generalize the notion of implicit requirements to include broader forms of changes in human experience and existence, by referring to the philosophical work on technological mediation. Applying this theory to electronic voting, especially Internet voting, I identify challenges that we need to face, should electronic voting come back on the political agenda.

24.2 Voting Requirements

Many different lists of requirements of voting systems exist. Although the categorization of the different desirable features varies, the intentions of the different sets overlap almost completely. The choice between the sets is therefore more or less arbitrary. Here, we use the requirements as compiled by the Election Process Advisory Commission of the Netherlands in 2007 (Adviesommissie Inrichting Verkiezingsproces 2007, pp. 20–21). It formulated the following requirements for elections, which we quote together with their explanation.

- Transparency—The election process should be organized in such a way that the structure and organization is clear, so that everyone in principle can understand it. There must be no secrets in the election process: questions must be able to be answered, and the answers must be verifiable.

- Verifiability—The election process should be objectively verifiable. The verification tools may differ, depending on the method of voting that is decided upon.
- Fairness—The election process should operate in a proper manner, and the results must not be capable of being influenced other than by the casting of lawful votes.
- Eligibility to vote—Only persons eligible to vote must be allowed to take part in the election.
- Free suffrage—Every elector must be able to choose how to vote in complete freedom, free from influence.
- Secret suffrage—It must be impossible to connect the identity of a person casting a vote to the vote cast. The process should be organized in such a way that it is impossible to make a voter indicate how he or she voted.
- Equal suffrage—Each voter, given the Dutch election system, must be allowed to cast only one vote in each election, which must be counted precisely once.
- Accessibility—Voters should be enabled as far as possible to participate directly in the election process. If this is impossible, there must be a way of taking part indirectly, i.e., by proxy.

Of these, the requirements of verifiability and free and secret suffrage are said to be the most challenging in combination. In order to protect the voter from bribery and coercion, an election must be 'receipt-free' (Benaloh and Tuinstra 1994). This means that it should not be possible for the voter to prove what her choice was. However, in order to verify the results, it must be assessable that each vote was counted as cast.

24.3 e-Voting in the Netherlands

One of the first European countries to introduce electronic forms of voting was the Netherlands (Pieters and van Haren 2007). Electronic voting machines were introduced during the 1990s, and appeared in the vast majority of polling stations. Most of these were manufactured by the Dutch company Nedap, and were so-called full-face direct recording electronic machines. Full-face means that all candidates are represented on different buttons on the machine. In 1997, a list of requirements was published that the machines would have to meet. Most of these are related to the required functionality under normal circumstances or robustness in case of failures. Few items are related to security, for example: 'The method of vote storage does not offer possibilities to derive the choice of individual voters' (translation by the author).[1] The voting machines had to be tested against the requirements by an evaluation institute.

[1] 'Regeling voorwaarden en goedkeuring stemmachines' 1997: 'De wijze van vastlegging van de stemmen biedt geen mogelijkheden tot vaststelling van de keuze van afzonderlijke kiezers'.

Although some criticism against the use of the machines had existed, the first systematic effort to challenge their legitimacy came from the pressure group 'Wij Vertrouwen Stemcomputers Niet' (We Don't Trust Voting Computers), established in summer 2006. After the founders had to vote on a touch-screen based system in Amsterdam, they were eager to demonstrate security and verifiability problems. To this end, they managed to purchase a couple of Nedap machines and analyzed their contents. They found out that it was rather easy to replace the program chips with ones that counted fraudulently. Since there was no way to verify the results, such attacks could go unnoticed. Moreover, they showed that it was possible to distinguish votes for a particular party by listening to the radio signals inadvertently emitted by the machine (Gonggrijp et al. 2006).

Whereas the verifiability was their main concern, the radio signal problem was most prominent in media coverage. The government was hesitant to change anything at first, but after independent commissions had investigated the problems (Hermans and van Twist 2007; Adviesommissie Inrichting Verkiezingsproces 2007), the legislation allowing electronic voting machines was withdrawn. New machines that would print the voter's choice on paper and then scan it were not built, because this design would not solve the radiation problem. Because this problem had been dominant in media coverage, and because the law and international treaties demand a secret ballot, e-voting in polling stations has been on hold since.

In the meantime, some experiments with Internet voting for expats and for water board elections had been run. After the problems with the electronic voting machines, security issues with these systems were considered enough reason to stop these experiments too.

It would be easy to explain the problems with electronic voting in the Netherlands in terms of security issues with the particular systems used. However, this would move our view away from more fundamental challenges of electronic voting. If electronic voting will come back in some form in the future, it is wiser to address these questions based on the information we have now gathered about electronic voting in practice. I will do so in the following sections.

24.4 Implicit Requirements

In the discussion on electronic voting in the Netherlands, two issues were crucial. First of all, what the pressure group put on the agenda was that whereas the machines were tested, the results of an individual election were unverifiable. The latter meaning of verification was never implemented in the requirements. Whereas with a ballot box, it may be reasonably assumed that—under controlled circumstances—what goes in is what comes out, this does not necessarily hold for electronic devices. Secondly, the machines emitted radiation in the casting process that could endanger the secrecy of the vote. Whereas the requirements state that

the secrecy should be maintained in storing the vote, the same issue had not been written down for casting.

We see that the discussion revolved around two implicit requirements: secrecy in casting, and verifiability of the results. Although it is generally agreed upon that these requirements make sense, they were not considered when the regulation was drawn up. Both are security issues: they are about limiting the possibilities for attackers to influence the result of the election. Why are such requirements often overlooked?

Requirements related to security are usually not functional requirements. They do not specify how a certain input should be transformed into an output. Instead, security requirements are about what should not be possible. An exception to this may be the requirement of verifiability, which is often thought of as a security requirement, but also specifies additional functionality. However, the primary goal of verifiability is still to limit the possibility of unwanted interference with the system.

Protection of technology is realized by means of causal insulation between the system and the environment (Luhmann 2005). Protection amounts to keeping unwanted causes out of the system and also preventing the system from having unwanted effects on the environment. In computer science, these properties are related to security requirements such as confidentiality and integrity, and the insulation property is called non-interference. However, whereas we may know perfectly what we want to achieve with the technology, there will undoubtedly be side-effects that we may wish to control, but that we are not necessarily aware of. That explains why security requirements often remain implicit. The problem is that whereas we would be able to argue convincingly that the technology being developed should not do this and this, we don't even know that it can do that.

The ways in which it is made sure that technology cannot do certain things are different depending on the type of technology. In physical security, we are used to working with walls, doors, and locks to limit access and thereby limit unwanted outside influences. In digital security, we often resort to cryptography and firewalls. The security properties of the digital and physical world are not necessarily the same. For example, a physical ballot box protects ballots by guaranteeing that nothing can go in or out without being observable. Based on what is common knowledge about physics, we can safely assume that this property is indeed realized. Ballots cannot just be copied inside the box. Such properties, however, are much less trivial in a digital ballot box. There, copying is easy to achieve, both because copying digital information does not require physical matter to be added and because computers contain active parts (programs) rather than passive matter only.

This is related to the distinction that was drawn by the Dutch pressure group between (mechanical) voting machines and voting computers. The former have a designated task that can be set in motion by pulling a handle. Manipulating the machine would amount to changing the inner mechanics. Computers, by contrast, can be programmed to perform tasks, and the tasks to be executed can be changed on demand. If the tasks are programmed correctly, they will usually be performed more reliably by the computer than by humans. However, it is hard to verify that a program will indeed do what it was intended to do. Even if computer programs are more reliable than humans, they may be less trustworthy (Pieters 2006a).

In existing (physical) technology, such as paper voting, such requirements may be realized in subtle ways, and the function of these mechanisms in terms of causal insulation may not be known anymore. When digitalizing such procedures, these mechanisms may be overlooked in the requirements elicitation process. For example, the role of the ballot box in safeguarding the verifiability of elections may not be perceived as such when requirements are drawn up for automated voting systems. In the words of Bruno Latour, these features are *blackboxed* (Latour 1999).

Thus, when changing the technology used in a domain such as elections, there may be hidden security measures in the original implementation, which remain implicit when writing down the requirements for the new technology. In electronic voting in the Netherlands, the most prominent ones were verifiability of the election results and secrecy of the vote when it is cast. Still, such implicit requirements are not necessarily limited to security problems. When broadening the notion of implicit requirements based on work in the philosophy of technology, much more challenges appear.

24.5 The Theory of Technological Mediation

Traditionally, technologies were thought of as morally neutral means to achieve certain ends. In the early 20th century, some philosophers (notably Ellul and Heidegger) realized that there was more, and they analyzed technology as an autonomous force shaping society. Later that century, it was recognized that both these views treat technology as a too uniform phenomenon. Rather than analyzing 'technology', these philosophers aimed to account for the role of concrete artifacts and technologies in our lives. It was recognized that humans and technology shape each other mutually, rather than one shaping the other.

In this 'empirical turn' in philosophy of technology, one of the movements drew its inspiration from the philosophical tradition of phenomenology. Whereas traditional phenomenology suffered from many of the same problems as the abstract philosophies of technology, the central insight—the relation between man and his environment is more fundamental than either of the two poles—turned out to be helpful in analyzing technological changes. A human being is always directed towards the environment, and this directedness is called intentionality. From this perspective, it is said that technology mediates the relationship between man and his environment (Ihde 1990; Verbeek 2005).

This mediation can take place at different levels and in different directions. Ihde (1990) mainly focuses on the mediation of human experience by technology, and distinguishes between micro- and macroperception. Mediation of microperception for example occurs when we look through a binocular: certain aspects of the world are amplified while others are reduced. In a more symbolic sense, this may also be said of the (mobile) phone: we experience the presence of other people in a

different way when we communicate by telephone. Here, the transformation is related to the direct perception by the individual.

Mediation of macroperception occurs when the cultural framework of perception (also termed 'cultural categories'; Smits 2006) is changed by the introduction of a technology. In earlier work (Pieters 2003), I discussed how technologies may mediate our idea of what nature is. The example I brought forward is the building of an ecoduct, connecting separated natural areas by a bridge over the interfering infrastructure. Apart from achieving something for nature, the building of such artifacts also has a different effect: it amplifies our interpretation of nature as a network of connected pieces. There is a mutual reinforcement going on between the understanding of nature as a network and the building of things that conform to this idea.

Verbeek (2005) introduces the existential direction of mediation in addition to the hermeneutical one explained above. Besides mediating experience, technology may also mediate our actions and the way we realize our existence. For example, the mobile phone not only changes our experience of appointments, but also the way in which we make appointments. Similarly, at a micro-level, a speed bump can mediate the way we drive.

In addition to the distinction between micro- and macro-level, I suggested adding a third 'meso'-level in earlier work (Pieters 2003). This would then correspond to matters of identification (hermeneutic) and orientation (existential), which both imply a sense of direction and are related to our habits. These notions were introduced by Christian Norberg-Schulz (2000) in his phenomenology of architecture. Examples of meso-level mediation are the mediated experience of nature by marked routes or GPS. This form is different from both microperception, where it is direct sensory perception that is mediated, and also from macroperception, since the mediation is not necessarily related to conceptual representations of nature.

The changes that a technology induces in its environment may be considered the scope of a broader notion of implicit requirements. Many requirements in terms of technological mediation would also be things that we do not want the technology to do. They are, however, less related to the manipulation of the functionality of the technology, and more to what the technology does to the people using it. In this sense, such requirements are related to a precautionary approach to the introduction of new technologies with respect to the users (Pieters and van Cleeff 2009). In the following, we will discuss the possible effects of technological mediation by voting technology.

24.6 Technology Mediates Voting

On a micro level, changes in technology may influence voter experience and behavior. For example, the butterfly ballot used for punch card technology in Orange County, Florida, in 2000, supposedly caused some people to vote for Pat

Buchanan instead of Al Gore. In the Netherlands, the line-up of candidates of a single party in two columns made it more likely that people voted for the number 31 instead of the number 1 of the list.

In countries using proportional representation, the full ballots listing all the candidates are often considerably large. In order to implement voting on a computer, phased voting may be introduced, in which people first choose a party and then a candidate. An interesting empirical question is how such an arrangement influences voting behavior, and thereby election results. This issue becomes even more critical when the ballot would have to fit on a mobile phone screen, or when people have to enter codes that correspond to candidates for SMS voting. Such mediations of the voting experience by voting technology should be investigated when new technologies are introduced.

In case of voting, identification and orientation on the meso-level have a political meaning. They are related to how one identifies oneself politically, and how one relates to the political environment. Both may be mediated by the environment in which the vote is actually cast. This may include features of the technology itself as well as the place where the technology enables the vote to be cast. For example, Oostveen and van den Besselaar (2005) suggest that people may vote differently depending on their trust in the technology used. Also, one can imagine that people would vote differently at home than in a polling station. Here, the mediation is not on the level of unconscious changes in one's voting behavior, or unintended mistakes. Instead, the voting environment makes one want to have a different political identity and want to vote differently.

In voting technology and democracy, similar things may happen as in ecoducts and nature on a macro-level. If voting systems are built with certain properties, and they seem to function reasonably well, this may reinforce the perception that such properties are good in general, thereby modifying our idea of what elections are and what democracy is. In this way, voting technology poses challenges to our cultural categories, which we term categorical challenges.[2] Several examples of such challenges will be presented in the next section.

24.7 Challenges

24.7.1 Voting System

Because computers can count more reliably, it becomes possible to use more complicated counting schemes for votes. Examples of such schemes are preferential voting methods, such as Single Transferrable Vote (STV). In STV, a voter can rank candidates in order of preference, and if her preferred candidate either already has enough votes or is eliminated, her vote goes to her next ranked

[2] In earlier work, I used the synonymous notion of conceptual challenge (Pieters 2006b).

candidate. This scheme is used in parliamentary elections in Ireland and Malta, and several local elections throughout the English-speaking world. It is argued that these more complicated schemes, although harder to understand, may increase the fairness of the electoral process, because votes are less likely to be 'wasted'. It can be expected that if automation of vote counting increases, the pressure to consider alternative counting schemes in other countries will also rise.

24.7.2 Autonomy

Already, the autonomy of the voter is being challenged by various voting adviser websites. At such sites, the voter can air her opinion on various political topics, and the site will provide and advice on which party or candidate to vote for. This takes politics from something that is about ideology to something that is about particular issues. In the hypothetical next stage, the voter may be given an advice based on her income and musical preferences. She may also be able to confirm her advice directly as her vote. Such arrangements, of course, are fundamentally incompatible with what we think of as making your own choice. Personalization of services is increasing (Van der Hof and Prins 2008), but this cannot be applied to voting without challenging the concept of voting itself.

Voting technology may itself contribute to such shifts in the conceptualization of what autonomy is in elections. Is the voter an autonomous rational individual, whom we need to isolate from emotional temptations in order to honestly provide her opinion? Or is the voter under constant influence of media, commercials and peer pressure, and may we as well allow her to vote from home? Traditionally, the walk or drive to the polling station and the associated procedures could be conceived as a ritual that confirmed her status as an autonomous citizen (Pieters and Becker 2005; Gerlach and Gasser 2009).[3] Such conceptual confirmations will be lost when remote voting is allowed, unless we are able to institute a new kind of ritual, which at least forces the voter to reconsider her choice in the same way as going to the polling station.

Another question is if the provisioning of autonomy to the voter requires equality of environment for all voters. Are elections only fair if each voter votes in a similar voting booth? Or can she vote through any channel of her choice? Obviously, elections were never fair in the sense that voting required the same effort of each citizen. Citizens who had a polling station around the corner were probably more likely to vote than those who would have to travel for miles. But, what if Internet voting allows some voters to cast their vote from their own computer, whereas their neighbors still have to travel to the nearest settlement? What do such unavoidable, but at least quantitatively variable, inequalities mean, for what we call the autonomy of the voter?

[3] See also Chap. 7 of this book.

Thus, voter autonomy includes both the decision to vote and the decision what to vote. In both senses, autonomy is always mediated autonomy, but we have to consider the role of voting technology in this mediation before we change to radically new devices.

24.7.3 Secret Ballot/Privacy

Although the secret ballot is now seen as a cornerstone of democracy, its introduction in the age of oral voting was far from trivial. Especially the discussion in England is well-documented (Asquith 1888; Gross 1898; Park 1931). It took 40 years, from 1832 to 1872, for the discussion to stabilize in the passing of a bill. Many felt that the secrecy of the ballot was 'inconsistent with the manly spirit and the free avowal of opinion which distinguished the people of England'. (Park 1931, p. 56). It was often thought that the ballot was 'un-English' and had never been used in the country, even though evidence was available for the contrary (Gross 1898). Against the main advantage, freeing the voters from coercion and other forms of influence, other counterarguments were raised.

> If there is ballot there can be no scrutiny, the controlling power of Parliament is lost, and the members are entirely in the hands of returning officers [officials responsible for elections, WP]. A representative will not be able to tell who his instructors are (i.e. the persons who elect him). People who do not wish to be suspected of voting on the wrong side will stay away. Ballot and universal suffrage are apt to be coupled, and universal suffrage will mean that the poor will gain everything and ruin everything. (Park 1931, p. 61).

One of the most important objections to the ballot, in light of current controversies on electronic voting, is the supposed lack of verifiability when using ballots. Votes cannot be traced back to the voter, so one cannot know by looking at a ballot if it is legitimate. The bill was only passed by the House of Lords in 1872.

Thus, opinions on ballot secrecy and verifiability shifted significantly during the 40 years of discussion. This also means that it would be possible that we might think quite differently about secrecy in elections, say, 50 years from now. How could voting technology affect such a shift?

The issue of secrecy in elections is related to the distinction between public and private environments. Traditionally, the home is a private environment, whereas politics takes place in a public sphere. However, to protect autonomy in the voting process, it was thought that a private environment was needed to cast a vote. This private environment was traditionally established by a voting booth at a polling station. By contrast, participation in political organizations such as parties was done publicly, but was judged to be a private matter. These complicated relations make it impossible to judge a secret ballot as a universal requirement of democratic politics.

Voting technology may influence the subtle relation between public and private in politics, especially when the place of casting the vote is changed with the

technology (as in remote voting). In remote voting, one is no longer provided a private space in a public environment, but rather acts in the unprotected public sphere at home, traditionally a private place. Therefore, the vote is not necessarily conceived as a secret act anymore. In terms of the public/private distinction, remote voting means a shift from a private moment in a public environment to a public moment in a private environment (Pieters and Becker 2005). Thus, voting technology may not only cause practical problems with the secrecy of the ballot, it may also change the association between voting and secrecy on a conceptual level.

In a more practical sense, there is the challenge how to maintain the secrecy and freedom of the vote in remote voting. One (partial) solution could be to allow voters to vote as many times as they like, where only their last vote counts. In this way, it is argued, voters could change their vote later, possibly even at a polling station, if they have felt pressure when casting their previous one. Again, this means a conceptual deviation from the idea that you can only vote once.

24.7.4 Verifiability

We have already seen that verifiability can mean two quite different things in voting: verifiability of the technology, or verifiability of the results. In future discussions on electronic voting, consensus must be reached about what is required for electronic voting to be acceptable. The discussion in the Netherlands suggests that verifiability of the technology alone is not enough.

When looking deeper into verifiability of the results, additional distinctions can be drawn. First of all, the literature provides a distinction between individual verifiability and universal verifiability. The former means that each voter can verify that her vote is included; the latter denotes the possibility to verify the results of the election based on the votes received. Both may be realized in two different ways: either the authorities 'prove' that they did their job correctly, without revealing the votes themselves, or they 'show' which votes they included and how they counted. In the latter case, results may be recalculated by independent parties. Note, however, that showing a voter her vote also introduces new opportunities for coercion. Earlier, I argued that the best combination would be to prove the inclusion of individual votes and to show (publicly) how the result was established (Pieters 2006c). This combination, however, proves to be difficult, and it may therefore be necessary to renegotiate desirable verifiability properties.

Another challenge introduced by verifiability features is what to do if somebody claims that something is wrong. If a voter can only say that the system shows the wrong vote, then there is no way to assess if she is legitimately challenging the system, for she may just have changed her mind in the meantime. Still, if many voters complain, the authorities may feel forced to do something. In such a case, disappointed voters may even start a coordinated action to undermine the established result. If a voter could really prove that her vote was registered incorrectly, then there is the possibility that an entire election needs to be re-run due to a single

challenge. Again, the desirability of these options needs to be evaluated, not only from a practical perspective, but also with respect to how they change electoral concepts.

24.7.5 Example: Estonia

To illustrate the subtle conceptual shifts, we briefly look at the developments in another country. Estonia allowed Internet voting for all citizens from 2005. The main theme in the Estonian discussion on remote voting was coercion-resistance versus equality. People might be coerced or tempted to sell their votes in an unsupervised environment. In order to limit the secrecy and freedom problems of remote voting, it was thought appropriate to allow remote voters to change their votes as many times as they wished, including overriding the remote vote in a polling station on election day. In this way, a coercer would need to have control over her victim all the time to be certain of compliance. This regulation was specified in the 2005 amendment.

> The right to change one's e-vote creates a so-called virtual voting booth: [a voter who has e-voted] under undesirable influence, can choose a moment when he or she is free to vote without outside influence. In order to guarantee freedom of voting, it is advisable to have the right to change one's vote on election day. With the same amendment, the Penal Code was also changed to exclude changing electronically given votes from punishable offenses. (Madise, et al. 2006, p. 19).

This partial solution to the problem of the secrecy and freedom of the vote can only work under a teleological interpretation of the requirement of secret voting in the constitution, i.e., that this requirement should be interpreted in terms of the problem it was meant to solve. Different means to guard against coercion would therefore also be appropriate. Also, the assumption was made that it was not primarily a task of the state to protect an individual against herself, so that collective voting and vote buying would not be a problem that needed solving (Drechsler 2003, pp. 4–5).

However, some people, among whom president Arnold Rüütel, had a different problem with the new arrangements. They felt that those gave unfair benefits to the remote voters. It would allow e-voters to change their mind in the period between advance voting and election day, but not those who voted in advance by other means. The president refused to sign the law. The parliament then made another amendment, removing the opportunity to change one's vote on election day itself. The president again refused cooperation, and appealed to the Supreme Court to have the act declared unconstitutional. The Court, however, ruled differently.

> The principle of uniformity cannot be interpreted as a requirement that all voters must in fact vote in a similar manner. Uniformity means, first and foremost, the requirement that all voters have equal possibilities to influence the voting result. (Decision of the Supreme Court of Estonia, quoted in Madise, et al. 2006, p. 25).

Uniformity of means of voting may no longer be a requirement of elections in Estonia. Election technology has thus mediated electoral concepts.

24.8 Conclusions

The technology that is used to implement the election process is not merely a means to achieve a pre-defined end. There may be implicit requirements that the technology does not meet, thereby shifting the requirements themselves in a direction that is favorable to the technology already implemented. Due to technological mediation, people may experience the voting process differently, and they may also make different choices depending on the environment in which they vote. No environment is completely neutral, but technology may cause a significant change, especially if the technology also implies a change in the place where the vote is cast. On micro- and meso-levels, such mediation may change the outcome of elections. On a conceptual level, the technology used may influence the cultural categories that form our understanding of voting and democracy. It is therefore necessary to identify as many implicit requirements as possible before moving to a new technology.

The main categorical challenges that we face in a possible future transition to electronic voting are:

- How to count the votes.
- How to conceptualize and realize voter autonomy.
- How to conceptualize and realize the secret ballot.
- How to conceptualize and realize verifiability.

All these concepts are subject to mediation by technology, and if we change the technology without thinking about these concepts, the mediated concepts may change us, instead of the other way around.

Acknowledgments This chapter is based on the author's PhD thesis La volonté machinale: understanding the electronic voting controversy, written at Radboud University Nijmegen (Pieters, 2008). The author wishes to thank Bart Jacobs for useful comments on a draft of this chapter.

References

Adviesommissie Inrichting Verkiezingsproces (2007) Stemmen met vertrouwen [Voting with confidence]. Den Haag, Adviescommissie inrichting verkiezingsproces. http://www.minbzk.nl/contents/pages/89927/advies.pdf

Asquith HH (1888) The ballot in England. Polit Sci Quart 3:654–681

Benaloh JC, Tuinstra D (1994) Receipt-free secret ballot elections (extended abstract). In Proc. 26th ACM Symposium on the Theory of Computing (STOC), ACM, pp 544–553

Drechsler W (2003) The Estonian e-voting laws discourse: Paradigmatic benchmarking for central and Eastern Europe. http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan009212.pdf

Gerlach J, Gasser U (2009) Three Case Studies from Switzerland: E-Voting, Berkman Center Research Publication No. 2009-03.1 Harvard University

Gonggrijp R et al (2006) Nedap/Groenendaal ES3B voting computer: a security analysis. http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf
Gross C (1898) The early history of the ballot in England. Am Hist Rev 3:456–463
Hermans LMLHA, Van Twist MJW (2007) Stemmachines: een verweesd dossier. Rapport van de commissie besluitvorming stemmachines. Den Haag, Commissie Besluitvorming Stemmachines. http://www.minbzk.nl/contents/pages/86914/rapportstemmachineseenverweesddossier.pdf
Ihde D (1990) Technology and the lifeworld. Indiana University Press, Bloomington
Latour B (1999) Pandora's hope: essays on the reality of science studies. Harvard University Press, Cambridge
Luhmann N (2005) Risk: a sociological theory. Transaction Publishers, New Brunswick
Madise U, Vinkel P, Maaten E (2006) Internet voting at the elections of local government councils on Oct 2005. http://www.vvk.ee/english/report2006.pdf
Norberg-Schulz C (2000) Architecture: presence language and place. Skira, Milan
Oostveen AM, Van den Besselaar P (2005) The effects of voting technologies on voting behaviour: issues of trust and social identity. Soc Sci Comput Rev 23:304–311
Park JH (1931) England's controversy over the secret ballot. Polit Sci Quart 46:51–86
Pieters W (2003) A pragmatic phenomenological approach in environmental planning. Master's thesis, Philosophy of Science, Technology and Society. Enschede, University of Twente
Pieters W (2006a) Acceptance of voting technology: between confidence and trust. In: Stølen K et al (eds) iTrust 2006. Springer, pp 283–297. Lecture Notes in Computer Science vol 3986
Pieters W (2006b) Internet voting: a conceptual challenge to democracy. In: Trauth et al (eds) Social inclusion: societal and organizational implications for information systems: IFIP TC8 WG8.2 International Working Conference. Springer, pp 89–103
Pieters W (2006c) What proof do we prefer? Variants of verifiability in voting. In: Workshop on Electronic Voting and e-Government in the UK. Edinburgh, e-Science Institute, pp 33–39
Pieters W (2008) La volonté machinale: understanding the electronic voting controversy. PhD thesis, Radboud University Nijmegen
Pieters W, Becker MJ (2005) Ethics of e-voting: an essay on requirements and values in internet elections. In ethics of new information technology: proceedings of the sixth international conference of computer ethics: philosophical enquiry (CEPE2005). Centre for Telematics and Information Technology, Enschede, pp 307–318
Pieters W, van Cleeff A (2009) The precautionary principle in a world of digital dependencies. IEEE Comput 42:50–56
Pieters W, van Haren R (2007) Temptations of turnout and modernisation: e-voting discourses in the UK and the Netherlands. J Inf Commun Ethics Soc 5:276–292
Smits M (2006) Taming monsters: the cultural domestication of new technology. Technol soc 28:489–504
Van der Hof S, Prins C (2008) Personalisation and its influence on identities, behaviour and social values. In: Hildebrandt M, Gutwirth S (eds) Profiling the European citizen: cross-disciplinary perspectives. Springer, Chapter 6, pp 111–127
Verbeek PPCC (2005) What things do: philosophical reflections on technology, agency and design. Pennsylvania State University Press
Vollan K (2005) Observing electronic voting, Technical Report 15. NORDEM 2005. http://www.humanrights.uio.no/forskning/publ/nr/2005/1505.pdf

Part VIII
Synthesis

Chapter 25
A Brave New Government?

Corien Prins and Wim Voermans

Abbreviation

ANPR Automatic number plate recognition

Contents

25.1 Introduction 456
25.2 The Concept e-Government 456
25.3 Making e-Government Work 458
25.3.1 Getting Connected 458
25.3.2 Identity Construction 461
25.3.3 Efficient Big Brother 463

Contribution received in 2010.

C. Prins (✉)
TILT – Tilburg Institute for Law, Technology and Society, Tilburg University, Tilburg, The Netherlands
e-mail: j.e.j.prins@uvt.nl

C. Prins
Scientific Council for Government Policy, The Hague, The Netherlands

W. Voermans
Department of Public Law, Leiden University, Leiden, The Netherlands
e-mail: w.j.m.voermans@law.leidenuniv.nl

W. Voermans
Meijers Institute for Legal Studies, Leiden, The Netherlands

S. van der Hof and M. M. Groothuis (eds.), *Innovating Government*, Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_25,

25.3.4 IT as a Tool for European Integration 464
25.4 Redefining Government 464
25.4.1 Changing the Face of Government: Seeing it in a Different Light 464
25.4.2 Accountability 465
25.5 Conclusion 466
Reference 466

25.1 Introduction

Whichever way we look at it, our governments radically change under the influence of technology. As a result, our lives in interaction with public sector bodies are easier and more agreeable. Services improve, communications run more smoothly. However, without a doubt the creation of an electronic government (e-government) also makes us more vulnerable and more dependent: dependent not only on technology itself, but also on the organizations within government that either apply technology, collect, and use citizen-related information or demand of citizens to submit themselves—voluntarily or not—to technological applications and their effects. And, government itself changes face at well. Throughout the centuries technology has proved capable of having an enormous influence on the way our society works and functions. Innovations in printing, shipping, and industrialization have shaped and framed our concept of politics and government–citizen relationship. In ways we only begin to understand today, but did not always do at the time. That is precisely why the social implications of the use of technology by government demand that choices are made. Choices made not only by individual public sector bodies, but also most certainly by people in politics, government, and actors involved in legislation. In the search for the guiding principles that are to be used as preconditions for these choices, we need to get an in-depth understanding of the developments related to electronic government. This book aims to contribute to this understanding.

In discussing and comparing the most prominent developments and issues reflected upon in the various chapters of this book, this chapter aims to support a further understanding of and knowledge on the dynamics of electronic government and hence, both the current and the future challenges of this endeavor. It is not our aim to summarize the book, but to present a synthesis of the findings by way of uncovering common threads in the contributions, to highlight topical issues, and explore future prospects.

25.2 The Concept e-Government

The first thing that comes to mind when considering the central theme of this book is what exactly defines e-government. And, how should we appreciate its relation with related concepts, such as e-governance? This appears an easier question to ask than answer. First, the contours of the concept are rather uncertain; there is not

a single definition of e-government. This is first and foremost due to the rapid development of ICT itself. Many different technologies could be considered under the *e* in e-government. In the earliest phase of development, the electronic dimension merely related to Internet and computer systems used in the administrative back-office. As is shown in many of the chapters in this book, other technological applications, such as Global Positioning Systems providing location-based services, Radio Frequency Identification, smartcards, and biometrics have become highly popular technologies because they are expected to offer numerous—even better—opportunities for e-government. Moreover, a wide range of very different types of activities by public sector bodies could constitute the broad domain of 'government.' The various contributions show these may be classified in four categories: care, control, service, and democracy. As a result, e-government is the umbrella term for such initiatives as e-publication, online filing, e-voting, policy trafficking, electronic surveillance, and personalized health services. In the broadest sense, the e-government concept nowadays also seems to include fulfilling the government's function to protect its people from terrorism and other kinds of crime.

Not only technology changes, but also the way government uses it as well. In the early days of the first decade of 2000, the concept of e-government was somewhat deterministic in nature: IT was thought of as a wholesome recipe for government and government services. That is why the UN defines e-government as a commitment by government to improve the relationship between the private citizen and the public sector through enhanced, cost-effective and efficient delivery of services, information, and knowledge. A UNPEPA 2002 report identifies different stages in this improvement process, starting with the establishment of a simple government online presence evolving into full integration of e-services across administrative boundaries (UNPEPA 2002). This definition is, in all fairness, a bit one sided. It does not yet fully acknowledge the way government itself changes face due to IT.

Where in the past the concept of e-government often appeared merely a perspective on newly available opportunities to realize smooth, effective, and efficient service delivery, and did not refer to the many other dimensions and challenges it may include, this perspective has changed in recent years. Ambitions in the domain of care and control are very much directed by new technologies and information processes. Hence, these days e-government is much more than a mere tool for efficient service delivery by public sector bodies. The discussions on biometrics (control) and e-health (care) in this book, testify to this development. And then of course there are new opportunities for a revitalization of democracy. In the past they were often reduced to e-voting, but today prominent attention is given to other opportunities, such as strengthening the overall legitimacy of government by means of e-participation, e-consultation, and e-petitioning. A glance at new web 2.0-based initiatives (for example those initiated under the US presidency of Obama) shows that the opportunities offered by inactive social networking applications appear highly interesting promises of e-government to ensure a better dialogue between agency policy makers and the public. However, with the advent

of web 2.0, government also faces the challenge of adapting new strategies for managing internal relationships. Values, such as taking initiative, open communication, and increased participation are becoming more and more important.

Government is affected in still different ways by ICTs in relation to citizens, economic operators, and civil society. We expect, indeed we demand, a different government in the IT-age. A more transparent and proactive government as regards information exchange and citizen participation. IT more and more challenges us to rethink processes and government relations. Of recent it triggers the re-engineering of government institutions itself. The legislative process, for instance, in a lot of countries changes face, embracing electronic legislative calendars, electronic consultation, and electronic promulgation (challenging the old ways of amending legislation). The process of voting itself is deeply affected, and governments seem to be ever more sensitive to the outcome of electronic polls which can be held with hitherto impossible, lightening speed.

In sum, governments across the world have widely recognized the potential of new ICTs to bring about fundamental renewal in not only internal government and public sector processes, but also their relationship with civil societal groups, the private sector, citizens, and various other actors. Both in the governmental relationship with citizens, civil society and businesses—for instance: democratic processes, public service delivery, or policy implementation; interorganizational arrangements—for instance: policy coordination, policy implementation, or public service delivery—and in intraorganizational activities—for instance: policy development, operational activities, or knowledge management—ICT offers a wide range of opportunities to increase efficiency, effectiveness, transparency, and participation.

The book is rich in contributions touching upon all these topics. In this chapter, we will—as announced—mainly focus on common threads and overall themes. To our minds these fall into two major categories.

I. IT enabling even improving government, including themes like interconnection, identification, improved service delivery, etc.
II. IT redefining government, i.e., changing government–citizen relationships (including identity, e-participation, and democracy), rule of law, and IT (including accountability).

25.3 Making e-Government Work

25.3.1 Getting Connected

A first tendency that can be distilled from the contributions is the urge to connect systems and data. A key ambition of governments in many countries is to share data, information, and knowledge across organizational boundaries in government administration. Illustrative initiatives can be found in several chapters. Van der Meer and Nouwt discuss developments in the healthcare domain that aim to

facilitate and improve the communication between professionals as well as to better inform patients and enhance their position. Information systems of individual healthcare providers are connected to national information infrastructures, establishing so-called Electronic Healthcare Records. Examples of the growing popularity to create so-called 'chains of information' can also be found in the domain of youth care. Here, interconnected systems are applied to allow for more effective information exchange between social work, schools, police, justice, and numerous other organizations across the country. Key aim is to prevent children—particularly those potentially at risk—from falling in between organizations and their systems once they move to another institution, school, professional, or municipality. The development is seen as instrumental in achieving a full integration of data on children, their emotional wellbeing, and social environment. A broad and integrated availability of data pertaining to the social and emotional development of children might prevent abusive situations for children and allow for timely and effective interference in damaging and unsafe contexts. The connection of information systems in combination with the application of risk-indication mechanisms to structure the exchange of data is seen as vital in proactively addressing present-day societal problems.

For sure, connecting information and knowledge allows for effective and efficient healthcare or youth care. Applying risk factors may support professionals in their awareness of looking for potential risks and problems. However getting connected may also have adverse repercussions for citizens and the professionals working with the systems. As is shown by van der Hof, the ambition to connect and interact is, e.g., prone to function creep, the incremental extension of functions of a system to other uses or contexts than those initially intended or specifically imparted in public policy. Also, the use of risk factors in categorizing and labeling data subjects may have negative effects. The attributed risk labels form the basis for probability calculations that determine the likeliness of individuals—children, tax-payers, patients, criminals—to behave in a certain manner or to experience certain risks. As Ton Monasso describes in this chapter, these labels are often presented as pseudo-objective because they are based on research. However, they are also value-laden and may introduce blind spots in the behavior and actions of professionals. Moreover, the labels run the risk of taking on their own dynamics, amounting to what van der Hof calls 'abstraction of personal identities', i.e., a tendency of data, knowledge, and profiles constituting a 'reality' distinct from the daily life of a citizen.

Both van der Hof and Monasso warn that in connecting systems and introducing instruments to find the 'most adequate' or 'the correct' information in these chained systems, we need to be aware of the value-sensitive choices that are made along the way. This brings us to an observation related to the current data protection regime. In a sense, the aforementioned tendency requires that we shift our attention from individual sets of personal data toward the statistical models, labels, profiles, and the algorithms with which individuals are assigned to a certain group or 'identity.' At present, these models, labels, and algorithms are unavailable for public contestation. However, the interests of the individuals that are judged and

'governed' on the basis of these labels seem to require that they are made public. Let us discuss this point in some more detail. The development towards chained information systems shows that more and more personal data are not used and processed anew and in isolation. On the contrary, 'useful' information and knowledge goes beyond the individual exchange between a citizen and professional of a set of personal data. In 'giving' his or her personal data to a certain organization, the individual does not provide these data for use in an 'objective' context. Today, the use and thus 'value' of personal data cannot be seen apart from the specifics of the context within which these data are used. Processing of personal data in chains of organizations occurs within, and is often structured by, social and institutional settings. Thus, the question is not so much whether personal data are processed. They always are and will be. It is an illusion to think that the current data protection regimes will limit the use of personal data. Rather, the problem is how personal data are processed, in what context, and toward what end. Therefore, the focus of the discussion should move away from single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. Given the developments of connected systems and the use of risk and other intervention labels, the discussion about protecting personal data must become a discussion about how individuals are typified (upon what social ontology, with what goal?) and who has the instruments and power to do so. Therefore, protecting personal data in our present-day society assumes the capability to know and to control about typifying people. It requires the availability of instruments to enable awareness of the statistical models, profiles and algorithms that are used to generate knowledge about individual behavior, social and economic position, and the data impression that individuals are exhibiting to others.

However, the implications of 'getting everything connected' not only face us with challenges in the domain of privacy- and identity-related issues. Dag Wiese Schartum argues in his contribution that even where rather simple or 'basic' information such as administrative data, is exchanged and shared, challenging issues arise. In facilitating the exchange of data and thereby share information and knowledge across organizational boundaries, information systems need to work with standardized definitions based in interoperability frameworks. Linking systems requires more than merely connecting ICT. Essential prerequisites in addition to technical interoperability are organizational interoperability, legal interoperability, as well as semantic interoperability.[1] However facilitating this broader

[1] EIS 2.0 states that interoperability can be affected by 'differences in legislation in areas such as administrative law, identification and authentication, intellectual property rights, liability, privacy and data protection, public administration transparency relationships between public administrations, citizens, businesses and other IT actors, and the re-use of public sector information in base registries' (p. 34). Cf., European Commission, Directorate General for Informatics; Supporting the European Interoperability Strategy Elaboration, Final Report Phase 1—02/07/2009, Deloitte, Section 4.2.1.4.

perspective on interoperability and accommodating legal regimes for the rather formalized, closed and inflexible computerized information systems, is indeed a challenge. By nature, law has elements of flexibility, openness, and discretionary leeway. Adopting legislation that can be, more easily than today, transformed and implemented in computerized information systems requires us to formalize legal concepts and draft 'computer-friendly legislation.' However, as Schartum shows, it is far from easy to go the road of formalizing words and phrases used in legislation without clashing with important legal principles. A key challenge for the legislature as well as academia will therefore be to look for a middle course in which both legal principles and effective administration and information systems could be accommodated.

In the political and public debate the privacy discussion is almost always about the use of personal data by organization X or company Y. Actually, what is increasingly at issue is the actions of complex systems rather than the actions of individual, recognizable and concretely approachable government agencies, or businesses. Decisions about citizens are taken by chain partners within information systems. This implies that it is increasingly less easy to determine which government organization is responsible for this decision. Moreover, these chains and systems do not restrict themselves to the boundaries of the government. Numbers, reference indexes, and other technical applications facilitate public–private cooperation, which makes the surveillance of government actions more complex. And, in this world of chains and systems it is increasingly less easy for citizens to find their way to file a complaint against the responsible government authority. For a citizen this means that the 'tangible' government agencies are dissolving into complex chains of institutions which only communicate with citizens when the authorities see the need to it. The government is assuming the form of a seemingly infallible and efficient system instead of an organization with recognizable and knowable people. And then of course the crucial question is who, in this chain of collaborating parties, will (have to) take the responsibility for privacy guarantees or autonomy and freedom of choice for citizens. Who exactly can be addressed on measures that have to be taken concerning a careful use of technology and personal data, on how to deal with these data and their (often still unknown) risks, the regulations (for the protection of data) that still have to be given, quality guarantees, and other obligations?

25.3.2 Identity Construction

A subsequent observation that can be distilled from the contributions in this book is that the issue of privacy protection in an e-government setting is part of the broader challenge of identification. For as the use of digital communication and interaction spreads, public sector bodies need appropriate mechanisms to meet identification needs. And, the specifics of electronic communication require the use of other mechanisms than those applied in the physical world. In order to be

certain in an electronic environment that certain rights and obligations are rightfully attributed to citizens, it is necessary to implement certainty and transaction security requirements. In particular the different chapters that focus on biometrics and identification schemes show that the requirements and rules that govern the new identification practices in turn entail specific legal regimes and a focus on new vulnerabilities.

However, the interaction of identification interests and ICT developments provides the topic with a second dimension. As is shown in various chapters in this book, ICT applications allow for various new opportunities for identification: personalized, unique, and centralized. National identity cards with biometric applications appear to be highly popular on the policy agenda of various countries. Although in some countries the public and political attitude is (still) hostile to ideas such as a nationwide identity card, other countries appear to institute identification schemes that show a clear tendency toward central and unique instruments to link a person with a document or other identification mechanism. The developments discussed by both Sprokkereef and van der Ploeg in the area of biometrics, show that policy makers decided to take advantage of certain reforms to introduce a national identification scheme or used the backdoor of another policy ambition to realize a national database for identification purposes. Another example of this tendency is the Citizens Service Number in the Netherlands. The general and unique number makes cross-referencing of data contained in the various public sector registers a lot easier.

This brings us to the following observation. The present-day discussion on privacy and data protection is almost always—in our view, mistakenly—about the (in)correct use of isolated personal data of individual citizens or consumers. However, the users of these data have already moved on. They are usually not concerned with known data such as name, address, town etc. The relation between users of data and citizens or consumers has gradually become a relation between government/industry and type of citizen/consumer. Under the influence of the possibilities offered by technology, government policies, and business strategies are zooming in on a certain 'identity' of citizen or consumer. The context in which data are collected [which person with which (behavior) characteristics shows which preference in which situation and under which (social and economic) circumstances] is becoming increasingly clear and can therefore play a more prominent part in government's policy making and industry's decision taking. In short, for government and industry we are becoming recognizable and transparent in different 'identities.' The initiatives discussed in this book by van der Hof as well as Monasso are prominent illustrations. By means of digital reference systems in youth care various institutions which somehow play a part in young people's lives, can automatically exchange data about youths. In this way they assemble a picture of the type of youngster they need to keep an eye on: which youngster with which (behavior) characteristics runs which risks in which situation and under which (social an economic) circumstances? In which family in which combination and (social and/or ethnic) background can we expect a serious possibility of child abuse or other domestic violence? With the help of several indicators professionals

in youth care try to gain insight into the type of child running a type X, Y, or Z risk of possible future criminal behavior. It is their ambition to make a start with the most appropriate form of direct help, depending on the type of risk. The initiatives are often explained by the government as offering an instrument to help children at risk personally, timely, and effectively. However, the initiative also entails the creation of digitally supported categories of children for whom a specific government policy (including the corresponding specific rights and duties) is to be drawn up. One might even go a step further and argue that here our government—thanks to technology—is stereotyping and stigmatizing.

Categorizing certain groups of citizens has far-reaching consequences. People will start judging themselves and others on the basis of characterizations created by the government. Neglect, stigmatization, and discrimination are just around the corner. In order to prevent precisely these—usually insidious—developments it is of the utmost importance to keep a critical eye on hidden social implications in complex technological developments. When the application of technology or the use of new knowledge gained with the help of technology is at issue, it is the task of the government, given its protective function, to base its arguments for protective measures on a thorough and objective analysis of the technology in question.

25.3.3 Efficient Big Brother

The very fuel of any government is information. More and detailed information helps government to foresee, and consequently ward off risk and harm, and it also helps to tailor policies to problems and issues. Biometrics help with precise and careful verification of identities, electronic child files, or medical files are an avenue for the improvement of child care and protection or public health, new surveillance technique helps inspection and by this compliance. There are, however, dilemmas involved. An all knowing government is difficult to keep in check with legal controls that date from an altogether other era. Van der Hof labels these dilemmas under the heading 'Legitimate paths to right wrongs.' Especially the contributions on surveillance are interesting in this respect. Wood and Webster note that our societies are becoming 'surveillance societies' in which technology-mediated surveillance is becoming normalized across Europe. This affects the landscape of liberty, security, and citizen–state relations. Discussing new technologies of surveillance in children's services Garrett would rather speak of a 'surveillance state' than a surveillance society now that much of the debate is centered on the public sphere. Garrett observes that the surveillance state is spurred on by the preoccupation governments nowadays have with risk and security. This has prompted preemptive approaches rather than reactive ones. With it comes the problem that government cannot sit idly by once it knows. As a consequence the intrusiveness of government may grow, not by design but as a side effect. These dynamics are hard to pin down, that is why Garrett—like Adorno—feels there is a need to try

and ascertain how technology is imbricated within the relations that embrace it. Van Ooijens contribution on the nodal orientation in surveillance—i.e., focusing policing more on the surveillance of the infrastructure, meaning the flows of people, goods, money, and information that use the infrastructure to move from one place to the other, rather than individuals, gives graphic evidence of the many conundrums involved. Automatic number plate recognition (ANPR) for instance makes it possible to track and check hitherto unfathomable amounts of vehicles, but does catching a handful of criminals justify the 24/7 passing of all vehicles passing an ANPR-camera?

25.3.4 IT as a Tool for European Integration

When we page through the different contributions information technology seems to have become the technology of choice of the EU. The EU uses IT for border and migration control, harmonization (geoinformation), and implementation of its policies and legislation (e.g., the Services Directive or e-health initiatives). Aside from the straightforward benefits and effects IT has for EU policies, it is tempting to see a bigger dimension: integration deepens when member states and the Union are plugged into one another in information networks on the basis of which they make their policies. Maybe drinking from the same well fraternizes.

25.4 Redefining Government

25.4.1 Changing the Face of Government: Seeing it in a Different Light

IT touches at the heart of state–citizen relations, and in a variety of ways we do not detect or suspect right away. IT has been rampant within government for the better part of two decades now, but only in the last decade or so it has truly touched upon state–citizens relations through the use of interactive IT. Our political systems, constitutions, and the bulk of the law have been established in times with a different physical context. When for instance we take a look into the ways legislation is enacted and amended, one has to bear the dynamics of printing press in mind to be able to understand why amendments to the law are quite unintelligible for a layman or citizens, but make perfect sense as a set of detailed instructions to a printer in order to arrive at a authentic consolidated text. New techniques of amending and correcting texts allowing for input from different authors at the same time (via track changes for instance) make the old techniques seem redundant and antiquated in the eyes of some, while others still read important guarantees in the old methods. A first observation we want to make in this section—based on the

contributions—makes us look at government institutions with new lenses. It makes us question and assess political and legal institutions in a new light but also think through traditional concepts in law and fundamental rights to new relations. For instance the improved possibilities to access and gather information the Internet and IT offer, has spurred on new transparency demands on government. Internet polling raise the demands on democratic government; citizens want to actually partake in government, not because history has learned this is in the end better for society or the political system as such, but simply because they can. This feature of IT will undoubtedly deeply affect state–citizen relations although at this moment the direction of the development is hard to predict. First because we are only at the beginning and second because causes and effects between IT and government relations are hard to distinguish. Pieters demonstrates how IT transforms voting. Technology, like e-voting helps with efficient voting, but also—due to so-called technological mediation—can result in people experience the voting process differently and—ultimately—may lead them to different choices depending on the environment in which they vote. The same may hold true for the way in which policies are prepared, enacted, and enshrined in law.

25.4.2 Accountability

Characteristic for almost all issues discussed in this book is a focus on personalized services, data sharing, public–private partnerships, blurring boundaries between the public and private sector, and the almost unlimited power of knowledge that the government acquires by using new technologies and data generated by these technologies. This again results in a move from a vertical, program-driven model of public sector activity to a more horizontal, user-centric model, as is among others discussed by David Murakami Wood and Webster in their chapter on the normalization of surveillance. This move will gradually lead to a fundamental overhaul of the basic machinery of the public sector. However, this new operational environment also changes the very relationship between trust and the object of accountability. The long-accepted model of accountability—the pyramidal conception of authority within government—needs to alter: the new setting in which administrative operations are now distributed horizontally between numerous actors, requires that accountability is attributed in a different manner. For it is problematic that, while systems and functions of different organizations start operating in a chain of linked systems, all these organizations retain their separate rights and obligations, and hence their own accountability regime. This raises concerns, e.g. connected with the transparency about who exactly can be held responsible and the citizens' ability to keep the participating public authorities under surveillance; this, too, challenges trust-building. Trust in large-scale comprehensive and interoperable chains of institutions and their systems therefore implies that accountability will have to be completely rethought so as to reflect the way government works.

25.5 Conclusion

The various chapters in this book all testify that government seems to have great confidence in technology and systems. For the time being there seems hardly any sign of a critical attitude toward the possibly vulnerable sides of all the systems. In many respects our society seems fascinated by all sorts of new technological applications and this will only increase. The consequences are obvious: new forms of vulnerability and citizens' dependence will arise. The human measure has disappeared. Moreover, it will become increasingly difficult to get a grip on the wider and long-term effects of the apparently autonomous dynamics of applying new technology. Of course, technology is a fact of life. However, the use of technology also goes hand in hand with new dynamics in the relationship between government and its citizens. It is therefore essential that the responsible actors are more concerned with questions regarding the relationship between different actors and, in particular, the relationship between governments and citizens. What kinds of shifts are taking place regarding power, position, and the shape of potential tools for government and citizens? Are the present social and political institutions and infrastructure in a position to deal with these trends and changes? Who should take responsibility and who precisely will be accountable for measures that have to be taken, how to deal with uncertain risks, the rules that have to be set, quality guarantees, and other obligations? In a world where technological applications play a dominant part we will have to weigh the promises on one hand and the possible risks of those applications on the other. Or do we, indeed, still look further in the future and—in all modesty—concede that it is still too early to tell what are the right responses to the problems. Are we fighting previous wars not aware of the way IT is affecting the heart of state–citizen relationships, unaware of a Brave New Government emerging?

Reference

UNPEPA (2002) United Nations Division for Public Economics and Public Administration and the American Society for Public Administration, Benchmarking E-government: a global perspective; assessing the progress of the UN member states