Reinventing Data Protection?

Serge Gutwirth · Yves Poullet · Paul De Hert ·
Cécile de Terwangne · Sjaak Nouwt
Editors

Reinventing Data Protection?

Springer

Editors
Prof. Serge Gutwirth
Vrije Universiteit Brussel
Center for Law, Science
Technology & Society Studies (LSTS)
Pleinlaan 2
1050 Brussel
Belgium
serge.gutwirth@vub.ac.be

Prof. Yves Poullet
University of Namur
Research Centre for Information
Technology & Law
Rempart de la Vierge 5
5000 Namur
Belgium
yves.poullet@fundp.ac.be

Prof. Paul De Hert
Vrije Universiteit Brussel
Center for Law, Science
Technology & Society Studies (LSTS)
Pleinlaan 2
1050 Brussel
Belgium
paul.de.hert@vub.ac.be

Prof. Cécile de Terwangne
University of Namur
Research Centre for Information
Technology & Law
Rempart de la Vierge 5
5000 Namur
Belgium
cecile.deterwangne@fundp.ac.be

Dr. Sjaak Nouwt
Royal Dutch Medical Association (KNMG)
Mercatorlaan 1200
3528 BL Utrecht
Netherlands
s.nouwt@fed.knmg.nl
(formerly: TILT, Tilburg University, Netherlands)

ISBN 978-1-4020-9497-2 e-ISBN 978-1-4020-9498-9

DOI 10.1007/978-1-4020-9498-9

Library of Congress Control Number: 2009920948

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Foreword by Karel De Gucht, Deputy Prime Minister and Minister of Foreign Affairs of Belgium

Twenty-first century world citizens are living at the crossroads of an ever expanding network of international trade-, investment-, travel-, communications- and knowledge flows. Modern societies find their dynamism in the free flow and competition of ideas and the free access to a wide range of information channels and pluralistic media.

Citizens discover new ways to develop their fundamental freedoms. Travelling across the globe – which a Minister for Foreign Affairs also does quite often – mobile ICT-technology allows us to stay abreast of developments at home or elsewhere. Credit cards – with microchips – also allow us to pay bills in virtually every hotel in the world.

MIT Professor Henry Jenkins has even developed the notion of '*twenty-first century literacy*', based on the ability to read and write but also digital skills to participate socially and collaboratively in the new media environment. These include: *instant messaging, Myspace, sampling, zines, mashups, Wikipedia, gaming and spoiling*.

Citizens in the developing world too use technological advancements to their maximal benefit. The introduction of mobile telecommunication in Sub-Saharan Africa is a good example. Faraway regions reconnect with their capital and the rest of the country, on which they often depend for the delivery of basic services. In many villages, citizens can either rent a mobile phone or make use of a collective mobile phone. The creation of a '*Virtual Souk*' on the Internet is another good example. Hundreds of craftsmen – in fact mostly women – in Morocco, Tunisia, Lebanon and Egypt suddenly gained direct access to the global market. Their sales volumes soared and their profit margins rose significantly.

These developments – often driven by new technologies – also bring along new threats for the individual citizen and for our modern, open society: such as identity theft, discriminatory profiling, continuous surveillance or deceit. That is why we must protect ourselves against the illegal use and the abuse of sensitive knowledge, technology and skills.

Within Europe, the individual's right to privacy is firmly embedded in the *European Convention on Human Rights and Fundamental Freedoms* of 1950. The Council of Europe reaffirmed these rights in 1981 when it adopted *Convention 108 for the protection of individuals with regard to the automatic processing of personal*

data. Furthermore, the European Union established clear basic principles for the collection, storage and use of personal data by governments, businesses and other organizations or individuals in *Directive 95/46/EC* and *Directive 2002/58/EC on Privacy and Electronic communications*.

Nonetheless, the twenty-first century citizen – utilizing the full potential of what ICT-technology has to offer – seems to develop a *digital persona* that becomes increasingly part of his individual social identity. From this perspective, control over personal information is control over an aspect of the identity one projects in the world. The right to privacy is the freedom from unreasonable constraints on one's own identity.

Transaction data – both traffic and location data – deserve our particular attention. As we make phone calls, send e-mails or SMS messages, data trails are generated within public networks that we use for these communications. While traffic data are necessary for the provision of communication services, they are also very sensitive data. They can give a complete picture of a person's contacts, habits, interests, activities and whereabouts. Location data, especially if very precise, can be used for the provision of services such as route guidance, location of stolen or missing property, tourist information, etc. In case of emergency, they can be helpful in dispatching assistance and rescue teams to the location of a person in distress. However, processing location data in mobile communication networks also creates the possibility of permanent surveillance.

Because of the particular sensitivity of transaction data the EU adopted in March 2006 a *Directive on the retention of communication traffic data*. This Directive provides for an EU-wide harmonisation of the obligations on providers and for limits on retention periods from six months to two years. Use of traffic data for the purpose of police investigations of criminal offences is regulated by national law.

This brings me to the heart of the ongoing public debate about security and privacy, all too often presented as dichotomous rivals to be traded-off in a zero-sum game. However responsible liberal and democratic policy makers do not have the luxury to balance one against the other. Both are needed.

In a twenty-first century information society, the fundamental freedoms of the individual cannot be protected by opposing technological developments, nor by seeking to control the use of particular technologies or techniques. Such policy preferences reflect the determination of certain authoritarian regimes to cut their citizens off from the rest of the world. Reporters Without Borders published a list of 13 Internet black holes, among which were Belarus, Burma, Cuba, Iran, Syria, Tunisia and Uzbekistan. But China is also mentioned, as the *world's most advanced country in Internet filtering.*

Dan Solove has suggested that a more appropriate metaphor for Data Protection than Orwell's *Big Brother* is Kafka's *The Trial*. I tend to agree with him. The concern is of a *more thoughtless process of bureaucratic indifference, arbitrary error and dehumanization, a world where people feel powerless and vulnerable, without meaningful form of participation in the collection and use of their information*.

Recent academic literature (Taipale, NY Law School professor) highlights the potential of 'value sensitive technology development strategies in conjunction with

policy implementations'. Privacy concerns are taken into account during design and development. Technical features can be built in to enable existing legal control mechanisms and related due process procedures for the protection of fundamental freedoms of the individual. Technical requirements to support such strategies include rule-based processing, selective revelation of personal data and strong credentials and audits.

The *particular privacy concerns* most implicated by employing advanced information technology for proactive law enforcement are primarily three. First, the *Chilling effect* or the concern that potential lawful behaviour would be inhibited due to potential surveillance. Two, the *Slippery slope* or the tendency to use powerful – but very intrusive – tools for increasingly pettier needs until, finally, we find ourselves in a situation of permanent surveillance. And three, the potential for *abuse or misuse*.

Programming code can never be law but code can bind what law, norms and market forces can achieve. Technology itself is neither the problem nor the solution. It presents certain opportunities and potentials that enable or constrain our public policy choices.

New technologies do not determine human fates: they rather alter the spectre of potentialities within which people act. An inter-disciplinary public debate is needed. Data protection is ultimately the shared responsibility of the individual, twenty-first century citizen, technology developers and policy makers together, next to that of data protection commissioners.

Karel De Gucht

Preface

In November 2007, the 'law and technology' research centres LSTS from the Vrije Universiteit Brussel, CRID from the University of Namur and TILT from Tilburg University co-organized the successful *Reinventing Data Protection?* conference in Brussels.[1] The conference gathered 150 people from all sectors of activities: universities, international, European and national administrations, companies, civil society associations, data protection authorities etc. and all were ready and interested to discuss the future of data protection in a society where information systems increasingly determine our destiny and shape our relations with our environment of humans and non-humans.

One of the roles of a university, *a fortiori* in the human sciences, is definitely to be a facilitator and stimulator of open and straightforward debates in a context of robust and tested knowledge. Such a role is certainly not neutral, since it urges all the stakeholders to revisit the genealogy and foundations of societal concepts and values in order to reshape and reframe political and societal discussion. Our explicit goal was to collectively re-initiate and invigorate the debate on data protection and its main concepts and objectives. In our opinion this debate is crucial and urgent, since our relationships with our physical or virtual co-humans, with the society as a whole and with things (that become 'intelligent') have drastically changed as a result of the introduction of powerful, ubiquitous and vital technologies in our lives. Since societies steadily reshape and rebuild themselves, it comes as no surprise that a tool such as data protection is in need of reinvention.

Let us shortly elaborate on the various reasons we had for initiating such debate.

1. **Why this debate**? At first glance it appears that data protection today receives more recognition, particularly from a legal perspective. The recently adopted EU Charter of Fundamental Rights erects data protection as a new fundamental right on an equal footing with the freedom of expression or the right to a fair trial. Also, more and more national constitutions are amended with a separate right to

[1] The conference was also co-organised and supported by the VUB instituut voor PostAcademische Vorming (iPAVUB) and the Vlaams-Nederlands Huis deBuren. It was further supported by the European Commission, the Fonds voor Wetenschappelijk Onderzoek (FWO) and the Fonds National de la Recherche Scientifique (FNRS).

data protection next to the more classical right to privacy. But beyond this formal recognition of a new constitutional right, a lot of interrogations remain. Is there a need to rethink the foundations of data protection in today's information society? What are the relationships between the 'old' constitutional right to privacy and its new counterpart, the constitutional right to protection of personal data?

The EU Charter of Fundamental Rights can, as Rodotà writes, be considered as the final point of a long evolution, separating privacy and data protection: from that point of view, the reinvention of data protection is ongoing, or more precisely, starting now.

In their former work De Hert and Gutwirth[2] described privacy and data protection as different but complementary fundamental rights. In order to devise accurate and effective privacy and data protection policies they must remain sharply distinguished. For these authors, by default, privacy law protects the opacity of the individual by prohibitive measures (non-interference), while data protection, also by default, calls for transparency of the processor of personal data enabling its control by the concerned individuals, states and special authorities. While privacy builds a shield around the individual, creating a zone of autonomy and liberty, data protection puts the activity of the processor in the spotlight, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor's accountability. Opacity tools, such as privacy set *limits* to the interference of the power with the individuals' autonomy and as such, they have a strong normative nature, while transparency tools, such as data protection, tend to regulate accepted exercise of power by channelling, regulating and controlling. In their contribution De Hert and Gutwirth focus on the future of data protection, after its consecration as a fundamental right in the 2000 EU Charter of Fundamental Rights. Using Lessig's typology, the Charter should be regarded as a 'transformative constitution' rather than as a 'codifying constitution'. Of these two types, the transformative constitution is clearly the more difficult to realize, since it must act when the constitutional moment is over. This is a good reason to focus upon the current process of constitutionalisation of data protection by the European Court on Human Rights in Strasbourg and the Court of Justice of the European Communities in Luxemburg.

Next to this, Rouvroy and Poullet and Hosein endorse the need to enlarge and deepen the privacy debate: they see privacy as a prerequisite for a living and non discriminatory democracy. For Rouvroy and Poullet the fundamental right to privacy fosters the autonomic capabilities of individuals that are necessary for sustaining a vivid democracy, which notably presupposes the right to seclusion or to opacity. The importance of privacy today then derives from the support it provides for individuals to develop both reflexive autonomy allowing to resist

---

[2] De Hert P. and S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' (2006) in E. Claes, A. Duff & S. Gutwirth (eds), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, pp. 61–104.

social pressures to conform to dominant drifts and deliberative abilities allowing participation in deliberative processes.
Finally, the notion of human dignity is often invoked as the ultimate basis for the recognition of privacy. Several authors highlight that data protection legislation is grounded on important ethical values, human dignity being one of them. Identifying these values might help to correctly interpret data protection rules in a still changing context (Rodotà and Rouvroy and Poullet).

2. **Why this debate**? Our conference gave the floor to all stakeholders in the current process of reinvention of data protection. We considered this to be an urgent necessity because the new information society environment raises still more fundamental political, economical and ethical issues, which need to be addressed with tools and actions stemming from different horizons. Data subjects are not only concerned as (net)citizens, concerned about their fundamental liberties but also as adequately and inadequately profiled consumers and as monitored and tracked employees at the workplace and even at home. Data subjects claim for collective bargains and for being more associated and implied in the design of the information systems surrounding them. Data controllers are acting individually and collectively, ready to discuss with their counterparts, acting on behalf of data subjects.
Building on previous work[3] Raab and Koops seek to develop a policy actor-based approach to data protection problems by looking into the actors' roles from empirical and normative standpoints, by considering actors' relationships to each other and to the instruments, by considering the levels or arenas in which they participate and by seeking greater clarity about the processes that are involved. They finish with some suggestions for adapting some of the roles within the cast of various actors, including the role of technology developers that may positively contribute to the future of privacy protection.
Importantly, the EU Charter of Fundamental Rights has constitutionally endorsed the fundamental role of the data protection authorities (DPA's) not only to solve concrete litigations or to give opinions on specific draft legislations or decisions but above all to incite democratic debates on strategic and prospective issues and challenges and to feed the different actors' reflections. To bring those tasks to a good end, the data protection authorities must be enabled to act in complete independence. Hustinx convincingly shows that this independence is not only a question of legal and political status but it must be conquered through the provision of adequate means and with the support from other stakeholders.

3. **Why this debate**? Because we have to rethink and reinvent some of the concepts laid down by current data protection legislation.

   - Firstly, the different data protection legislations have been constructed upon concepts closely related to the nature of the data at stake (personal data v. non

---

[3] Bennet, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd edn.), Cambridge, MA: MIT Press.

personal data; sensitive data v. non sensitive data). However, it has clearly become even more obvious that if the prime concern is the preservation of the citizen's autonomy, the concept of personal data turns out to be problematic and no longer seems to be appropriate: surveillance societies work with profiles and technology that are able to detect or predict behaviour without necessarily processing personal data. As regards the profiling techniques used both by public authorities and private companies, Hildebrandt denunciates their reductionism and opacity, which destroys any possibility of self-determination for the citizens. To her, the focus on personal data must be complemented with a persistent focus on the dynamic profiles that will soon have more impact on life than trivial or non-trivial data. Consequently, she holds a plea for the recognition of a right of access to profiles and of a right to contest the validity or the fairness of the application of a profile. To be effective, Hildebrandt contends, these rights need to be complemented with legal obligations for those that construct and apply profiles and they need to be inscribed in the technological infrastructure against which they aim to protect.

- Secondly, data protection legislation only takes into account a limited number of actors, focusing on data controllers and data subjects. But today technology and information systems are introducing new actors whose intervention create new risks: the terminal equipment producers and the infrastructure operators. How to address these new risks and how to assign an appropriate liability to these actors? Dinant points out that the Article 29 Working Group has recently stressed the 'responsibility for data protection from a societal and ethical point of view of those who design technical specifications and those who actually build or implement applications or operating systems'. This being said and proclaimed, is it socially acceptable that there is no well-defined legal liability for those actors?
- Thirdly, all data protection regulatory instruments, national legislation or international conventions, self-regulatory instruments or public regulations do implicitly refer to a common and universal list of minimal guarantees that already seem to have an universal character. Indeed, international privacy standards have already been defined for more than a quarter of a century, expressed in the OECD Guidelines and in the Council of Europe Convention 108. However, de Terwangne contends that the last international data protection instrument, the Asian-Pacific Economic Cooperation (APEC) Privacy Framework adopted in 2004, weakens these standards, even if it nevertheless expresses the expansion throughout the world of the concern about data protection. The development of the Internet has rendered this concern critical. ICT developments in general and the tremendous growth of their use in all human activities have also shown the necessity to enrich the fundamental data protection principles with additional principles meant to maintain the balance between the efficiency of the technological tools and the power of their users on one side and the rights and interests of the individuals, data subjects, on the other side.

- Fourthly, can we consider that the regulatory concepts of data protection legislation – consent and proportionality – put in place for limiting the data processors' right to collect and process information have to be renewed and rethought? Consent and proportionality indeed play a fundamental role for legitimizing their processing. Perhaps these concepts must be deeply renewed given, as Bygraeve and Shartum describe, that the 'consent' often turns out to be formal, rarely free and often unavoidable and that the principle of proportionality shows a persistent lack of teeth. Nevertheless, Brownsword fundamentally defends consent as a central concept in the data protection regime and he argues that data protection regimes should be based on right-based consent, rather than on duty-based confidentiality obligation. This is especially the case insofar as the information society evolves into an IT-enabling profiling community in which processing and profiling are carried out on a daily basis by much less visible operators. But for Brownsword there is more at hand: the option for a right-based approach, as opposed to dignitarian and utilitarian positions, fits into Europe's commitment to human rights: the consent of the right holders must stay as a cornerstone in data protection regime.
  Bygrave and Schartum explore if new forms of collective consent and new procedures to establish the proportionality of the data processing would be needed, since both consent mechanisms and the principle of proportionality suffer certain weaknesses. Mechanisms for *collective exercise of consent* are probably hard to realize under the present legal limitations. Yet the authors contend that collective consent could both bolster the position of the individual data subject towards data controllers and make proportionality as a principle guiding consent more likely.
  On this issue, Berkvens refers to the 'Consumer privacy Approach' adopted by certain recent new US-legislations: such an approach clearly favours collective agreements defining the conditions and modalities of the data processing. Such an approach would also recognise the importance of the consumer' education and information and lead to class actions that might enhance the effectiveness of data protection. Berkvens concludes by pleading for restarting the dialogue between the entrepreneur and the consumer.

4. **Why this debate**? How to face the new networked and global world wherein our relationships and actions become still more formatted by technological devices and a long list of diffuses economic, social and political interests? Undoubtedly, the normative instruments need to take into account such new characteristics through different means.

   - Attention must indeed be paid to ways to regulate privacy and data protection beyond the national borders. Self-regulation, for instance, offers methods to increase the effectiveness of data protection principles, such as labelling systems, privacy policies and Alternative Dispute Resolution mechanisms. Such ways offer credible complementary or alternative tools for the traditional legislative approach. The value of self regulatory instruments must nevertheless

be assessed according to certain criteria such as the legitimacy of their authors (since it is quite clear that the more the different stakeholders are represented in the drafting and evaluating process of these instruments, the more it will be difficult to dispute them), the degree to which they substantially comply with the Fair Information Principles and their effectiveness and enforcement mechanisms.

- If technology constitutes the risk, technology might well also offer a solution for protecting privacy. Pursuing this idea, Winn underlines the attention paid by the data protection authorities to standardisation bodies and the need for these private or public institutions to dedicate sufficient consideration to the privacy requirement in the definition of the norms. She explores the costs and benefits of trying to integrate technical standards into European data protection laws as a possible strategy to enhance compliance and enforcement efforts. Accepting the discipline imposed by 'better regulation' principles and adopting new perspectives on the legitimacy of regulatory bodies, might increase the chances that ICT standards can be harmonized with data protection laws, which in turn might increase the practical impact of those laws. Dinant briefly demonstrates how the transclusive hyperlinks feature, embedded in recent browsers, permits Google to tap in real-time a substantial part of the clickstream of every individual surfing on the net, even if not using the Google search engine. The call for a value-sensitive design of terminal equipments and of the infrastructure is in line with a new broad approach far beyond the limits of the data protection legislation.
- Trudel suggests a new approach founded on risk management, which turns down any dogmatic vision, be it the legislative interventionist or the liberal one. He convenes all the different stakeholders to analyse the risks involved and to assign the adequate remedy at each level of the information systems. From that perspective the author describes a 'networked normativity', which should be built up in a transparent way.
- It also means that the laws guaranteeing privacy and enforcing data protection must evolve as to fit the technological and socio-political evolutions generating new threats for the individuals' capacity for 'self-development' of their personality. According to the German Constitutional Court's opinion the development of the data processing technologies obliges the State to revise and adapt the guarantees it provides to the individuals in order to protect and foster the capabilities needed to implement their right to freely self-determine their personality. In the circumstances of the day, the legal protections offered to the individuals' capabilities for self-development would probably need to address the specific threats accompanying the development of ubiquitous computing and ambient intelligence, as stated by Rouvroy and Poullet, Hildebrandt and Rodotà.

5. **Why this debate**? Certain specific privacy issues are particularly pertinent and should be focused upon.

- Firstly, privacy is most certainly a fundamental liberty but its protection might hinder other liberties or prejudice security interests. Szekely analyses the possible conflicts between freedom of expression and privacy. According to the author 'privacy' and 'freedom of information' are neither friends, nor foes of each other but complementary concepts. However, both concepts have conflicting areas and Szekely discusses these areas from two perspectives: the private life of the public servant and the information about collaborators of former (dictatorial) regimes that could constitute 'data of public interest'. Furthermore, both information privacy and freedom of information have been put at risk by the restrictions in the post-9/11 era. Szekely concludes by proposing the use of a checklist for decision-makers that could help to limit the restrictions of information privacy and freedom of information to the extent that is both necessary and sufficient but also reversible.

  Next to the freedom of information the claim for security is often evoked to justify interferences and restrictions of the citizens' liberties. The need to maintain the priority to our liberties and to consider security as an exception that might be invoked only under strict conditions, justifies the adoption at the EU level of a framework agreement, which applies the same concepts in the third and the second EU pillars as in the first pillar. However, Alonso-Blas does not favour such an approach. To her, data protection in the third pillar area should of course be based on the common principles established in Convention 108 and further developed in Directive 95/46/EC but requires a careful consideration of the specific nature of personal data processing in this sector. The particular features of police and judicial work need to be taken into account: in fact, there is a need for very clear and specific tailor-made rules for the diverse areas of activity within the third pillar field.

  For Nouwt to protect personal data in the third EU pillar adequately, it is important to tune the economic data protection approach by the EU with the human rights approach by the Council of Europe. This could and should result in a common approach for data protection within 'the two Europes' and perhaps even beyond.
- Secondly, the global dimension of the information society obliges all the countries to adopt common rules at an international level in order to effectively protect privacy and personal data. This has recently been requested not only by the World Summit of the Information Society (WSIS) in Tunis but also by Google. On that point, de Terwangne opposes two approaches, namely the APEC self-regulatory model and the EU legislative model. The recent Council of Europe Convention on Cybercrime – opened to the signature of all countries, with growing success – definitively demonstrates that it is possible to find solutions suiting all actors. While waiting for this international consensus, the solution proposed by article 25 of EU Directive 95/46/EC as regards the Transborder Data Flows has however been firmly criticised. In Kuner's opinion, this legal framework is inadequate, in both a procedural and substantive sense and needs reforming. Kuner describes the procedural problems in a very original and mathematical way, concluding that

there are only 78 potential adequacy candidate countries and that it would take 130 years for these countries to be considered adequate. More substantially, the adequacy provisions are contained in a separate chapter in the Directive and are not part of the general rules on the lawfulness of the processing of personal data. Furthermore, it appears that in its adequacy decisions, the European Commission does not always require third countries to prohibit the transfer to non-adequate countries. Kuner concludes that for a number of reasons, an accountability or liability approach (accountability for the data controller) would be more efficient and effective than the adequacy standard.

As concluded by Burkert and by many of the contributions of this book, the constitutional acknowledgment of data protection as a fundamental right should be considered not only as an achievement but also and more important, as a new starting point. The recognition of the fundamental right to data protection is directed towards the future. It has a transformative stance and should create the opportunity of a dynamic participative, inductive and democratic process of 'networked' reinvention of data protection (rather than a contained and reductive legal exercise). We will be happy editors if the present book succeeds in contributing to the seizing of this opportunity.

In respect of the diversity of nationalities, disciplines and perspectives represented in this book, the editors and the publisher have left the choices concerning the use of reference systems and spelling to the authors of the contributions.

Serge Gutwirth
Yves Poullet
Paul De Hert
Cécile de Terwangne
Sjaak Nouwt

Contents

Contributors

Jan M. Berkvens is senior counsel at the legal and tax department of Rabobank Nederland and professor of law and informatics at Radboud University Nijmegen. His research focuses on legal aspects of information technology such as e-commerce and payment systems. He is an expert in data protection issues.

Diana Alonso Blas is the Data Protection Officer of Eurojust, the European Union's Judicial Cooperation Unit, since November 2003. She studied law at the universities of San Sebastián (Spain), Pau et les Pays de l'Adour (France) and Leuven (Belgium). Subsequently she followed a LL.M. European law postgraduate program at the University of Leuven where she graduated magna cum laude in 1993. From 1994 to 1998 she worked as research fellow for the Interdisciplinary Centre for Law and Information Technology (ICRI) of the Catholic University of Leuven (K.U.L.). In this same period, she spent one year acting as privacy expert for the Belgian Data Protection Authority in Brussels. In April 1998, she joined the Dutch Data Protection Authority where she was a Senior International Officer working under the direct supervision of Peter Hustinx until the end of January 2002. During this period, she represented The Netherlands in several international working groups, such as the article 29 Working Party and the Consultative Committee on Convention 108 at the Council of Europe. From February 2002 to November 2003, she worked at the Data Protection Unit of Directorate General Internal Market of the European Commission, in Brussels. She is author of numerous articles and reports dealing with data protection at European level in the first and third pillar and is often invited as speaker at European and international data protection conferences. She has also performed as guest lecturer at the universities of Tilburg (Netherlands) and Edinburgh (UK). She is a Spanish national and speaks five languages.

Roger Brownsword is a graduate of the London School of Economics. Since September 2003, he has been professor of law at King's College London and honorary professor of law at the University of Sheffield. He is director of a newly formed research centre (TELOS), based on the School of Law at KCL that focuses on regulation, ethics and technology.

Professor Brownsword acted as a specialist adviser to the House of Lords' Select Committee on Stems Cells and, more recently, to the House of Commons'

Science and Technology Committee for its report on hybrids and chimeras. Since Autumn 2004, he has been a member of the Nuffield Council on Bioethics; he was a member of the Nuffield Working Party on Public Health; and he was a member of the Academy of Medical Sciences' committee on Brain Science, Addiction and Drugs that reported in Summer 2008.

He has published some 200 papers; his latest books are *Rights, Regulation and the Technological Revolution* (OUP, 2008) and a co-edited collection, *Regulating Technologies* (Hart, 2008); and he is the general editor of a newly launched journal, *Law, Innovation and Technology*.

Herbert Burkert is professor of public law, information and communication law and president of the Research Centre for Information Law at the University of St. Gallen, Switzerland, and a senior researcher at the Fraunhofer Institute for Intelligent Analysis and Information Systems in Germany (currently on leave of absence).

Lee A. Bygrave (<http://folk.uio.no/lee>) is associate professor at the Law Faculty of the University of Oslo. He is also research associate (formerly co-director) of the Cyberspace Law and Policy Centre at the University of New South Wales, Sydney. His teaching appointments range across numerous institutions, including the universities of Vienna, Stockholm, Tilburg, New South Wales and Oslo. He has published extensively within the field of privacy/data protection law. He is the author of an international standard work in the field, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002). Bygrave has advised on privacy and information security issues for a broad range of organizations, including the European Commission, Nordic Council of Ministers, Norwegian Government, U.S. National Academies, U.K. House of Lords Select Committee on the Constitution, and Telenor. In 2007, he was appointed by the Norwegian Government to serve on a Privacy Commission that was tasked to assess the state of privacy protection in Norway and to propose measures for bolstering such protection. The Commission submitted its final report to the Government in January 2009. Much of Bygrave's current academic research focuses on Internet regulation. He has recently produced an anthology titled *Internet Governance: Infrastructure and Institutions*, which was published in early 2009.

Karel De Gucht is Deputy Prime Minister and Minister of Foreign Affairs of Belgium. He is also a professor of European law at the Vrije Universiteit Brussel.

Paul De Hert is professor of law at the Faculty of Law and Criminology of Vrije Universiteit Brussel. He is the director of the research group on Fundamental Rights and Constitutionalism (FRC) and senior member of the research group on Law, Science, Technology & Society (LSTS). He is also associate professor of law and technology at the Tilburg Institute for Law, Technology, and Society (TILT)

Cécile de Terwangne has a MD in law (University of Louvain), a PhD in law (University of Namur) and a LLM in European and international law (European

University Institute of Florence). She is professor at the Law Faculty of the University of Namur (Belgium). She teaches civil liberties, computer and human rights, and data protection. She is director of the post-graduate Program in Law of Information and Communication Technologies at the University of Namur. She is research director in the Freedoms in the Information Society Unit of the Research Centre for Computer and Law (CRID – University of Namur). She has taken part to numerous European and national research projects in the fields of data protection, privacy and ICT, freedom of information, e-Government, re-use of Public sector information, etc. She is director of the «Revue du droit des technologies de l'information» (R.D.T.I.).

Jean-Marc Dinant obtained a Master degree in computer science in 1985, after two years of economics. After various research projects in the field of expert systems, adults training and telecommunication networks, he has joined the Belgian Data Protection Authority in 1993. Since then he has worked in strong collaboration with lawyers in the data protection area. He has left the Belgian DPA in 1998 while remaining a technical expert inside the art 29 working party until 2001. Since 1994, he is working as a researcher in the Research Centre on IT and Law (CRID) of the University of Namur where he tries to be a full duplex gateway between lawyers and technician in the context of privacy and data protection. Within the CRID, he is currently head of the Technology and Security Unit and coordinates various research projects dealing with technology, security and privacy. Since 2001, Jean-Marc Dinant has been a technical data protection expert for many institutions including the Council of Europe and the European Commission. He is also a Member of the Belgian Association of Expert witnesses since 2003. He is currently senior lecturer at the University of Namur where he is teaching cyber security and ending his PhD in Computer Science about Privacy Enhancing Technologies.

Serge Gutwirth is a professor of human rights, legal theory, comparative law and legal research at the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB), where he studied law, criminology and also obtained a post-graduate degree in technology and science studies. He also holds a part-time position of lecturer at the Faculty of law of the Erasmus University Rotterdam where he teaches philosophy of law, since October 2003. He is holder of a 10-year research fellowship in the framework of the VUB-Research contingent for his project 'Sciences and the democratic constitutional state: a mutual transformation process'.

Gutwirth founded and still chairs the VUB-research group Law Science Technology & Society (http://www.vub.ac.be/LSTS). He publishes widely in Dutch, French and English. Currently, Serge Gutwirth is particularly interested both in technical legal issues raised by technology (particularly in the field of data protection and privacy) and in more generic issues related to the articulation of law, sciences, technologies and societies.

Mireille Hildebrandt is an associate professor of jurisprudence at Erasmus School of Law and Dean of education of the Research School of Safety and

Security in the Netherlands. She has written her PhD thesis on the principle of 'no punishment without trial', from the perspective of legal philosophy, anthropology and legal history. Since 2002 she has been seconded to the centre of Law Science Technology and Society (LSTS) at Vrije Universiteit Brussel, as a senior researcher and has been coordinator of profiling in the EU research consortium on the Future of Identity in Information Society (FIDIS). From 2007 to 2012 she works on a research project on 'Law and Autonomic Computing: Mutual Transformations', investigating the legal implications of ubiquitous and autonomic computing. Her research interests concern the impact of emerging and future ICT infrastructures on issues of privacy, autonomy, causality, agency, legal personhood and due process. She is an associate editor of Criminal Law and Philosophy and of Identity in Information Society (IDIS) and publishes widely on the nexus of philosophy of law and of technology, with special regard for criminal law. She co-edited (with Serge Gutwirth) and co-authored 'Profiling the European Citizen. Cross-Disciplinary Perspectives' (2008).

Gus Hosein is an academic, an advocate, and a consultant. He is a visiting senior fellow at the London School of Economics and Political Science where he lectures and researches on technology policy. He is a senior fellow with Privacy International in London where he co-ordinates international research and campaigns on civil liberties. He is also a visiting scholar at the American Civil Liberties Union, advising on international technology and liberty issues. Finally, he is a consultant to international, governmental, non-governmental, and private sector organizations on data governance, civil liberties, and privacy. He has a B.Math from the University of Waterloo and a PhD from the University of London. He is also a fellow of the British Computer Society (FBCS CITP) and a fellow of the Royal Society for the encouragement of Arts, Manufactures and Commerce (FRSA). For more information please see http://personal.lse.ac.uk/hosein.

Peter J. Hustinx has been European Data Protection Supervisor since January 2004. He has been closely involved in the development of data protection legislation from the start, both at the national and at the international level. Before entering his office, he was president of the Dutch Data Protection Authority since 1991. From 1996 until 2000 he was chairman of the Article 29 Working Party. He received law degrees in Nijmegen, the Netherlands, and in Ann Arbor, USA. Since 1986 he has been deputy judge in the Court of Appeal in Amsterdam.

Bert-Jaap Koops is a professor of regulation & technology at the Tilburg Institute for Law, Technology, and Society (TILT), the Netherlands. He is also a senior researcher at Intervict, the Tilburg institute for victimology and human security, and a member of *De Jonge Akademie*, a branch of the Royal Netherlands Academy of Arts and Sciences with 80 young academics.

His main research interests are law & technology, in particular criminal-law issues in investigation powers and privacy, computer crime, DNA forensics, and cryptography. He is also interested in other topics of technology regulation, such as information security, identity, digital constitutional rights, 'code as law',

human enhancement, and regulation of bio- and nanotechnologies. Since 2004, he co-ordinates a research program on law, technology, and shifting power relations.

Koops studied mathematics and general and comparative literature at Groningen University, the Netherlands. He did a PhD in law at Tilburg University and Eindhoven University of Technology with a dissertation on cryptography regulation in 1999. He has co-edited five books in English on ICT regulation and published many articles and books in English and Dutch on a wide variety of topics. Koops' WWW Crypto Law Survey is a standard publication on crypto regulation of worldwide renown. He gave invited lectures in the U.S. at the University of Dayton, Ohio, and George Washington University, Washington, D.C., and in the U.K. at King's College London.

Christopher Kuner is partner and head of the International Privacy and Information Management Practice at Hunton & Williams in Brussels. In 2007 and 2008, he was voted the 'go-to person for EU privacy' in a survey of leading privacy lawyers conducted by Computerworld magazine. Mr. Kuner is a member of the Data Protection Experts Group (GEX-PD) of the European Commission, and is author of the book *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2nd edition 2007), which has also been published in Chinese by Law Press China. He is Chairman of the International Chamber of Commerce (ICC) Data Protection Task Force and the European Privacy Officers Forum (EPOF), and guest lecturer in data protection and IT law at Vienna University of Economics and Business Administration.

Ronald Leenes is an associate professor in law and (new) technology and academic director of TILT, the Tilburg Institute for Law, Technology, and Society. Ronald has a background in public administration and public policy (University of Twente) and has extensive research experience in the fields of artificial intelligence and Law, E-Government and since he joined TILT, technology (primarily ICTs) and law. His primary research interests are regulation of and by technology, specifically related to privacy and identity management. He leads research teams in the field of privacy-enhancing identity management and Online Dispute Resolution. He is also involved in research in ID fraud, biometrics and e-government. He was/is work package leader in the EU FP6 PRIME project and the EU FP7 project PrimeLife. He has contributed to and edited various deliverables for the EU FP6 Network of Excellence 'Future of IDentity in the Information Society' (FIDIS), and he participated in the Network of Excellence 'Legal Framework for the Information Society' (LEFIS). Ronald is a productive researcher with a large number of international publications in books and (refereed) journals and refereed conference volumes.

Sjaak Nouwt is working as a policy officer in health law at the Royal Dutch Medical Association (KNMG: www.knmg.nl) in Utrecht (Netherlands) on topics related to privacy and ICT. From 1985 to February 2009, he was an assistant professor at the Tilburg Institute for Law, Technology, and Society (TILT) of Tilburg University, Faculty of Law. At TILT, he taught master courses in *Privacy*

and Data Protection, *Public Information Law,* and *Health Law.* In 1997, Nouwt published his doctoral thesis on the use of information technology in health care and the protection of medical data. He published several articles and (chapters in) books on privacy and data protection issues. He is editor-in-chief of a Dutch journal on Privacy and Information (*Privacy & Informatie*) and also of a Dutch journal on Data Protection in Health Care (*Journaal Privacy Gezondheidszorg*). Furthermore, he is a member of the editorial staff of several text-books, and loose-leaf publications on privacy and data protection. He is also a privacy consultant.

Isabelle Oomen joined the Tilburg Institute for Law, Technology, and Society (TILT) at the University of Tilburg as a junior researcher, after graduating from her sociology studies. She has conducted quantitative and qualitative research, as well as literature research, on privacy, identity, identity management, profiling, and e-government. Recently, Isabelle started her PhD research on privacy in online social networks. Her study is part of the project 'The Social Dimensions of Privacy' which is carried out by TILT and the University of Amsterdam.

Yves Poullet Ph.D. in law and graduated in philosophy, is full professor at the Faculty of Law at the University of Namur (FUNDP) and Liège (Ulg), Belgium. He teaches different topics like: 'Sources and principles of the law', 'Internet regulations', 'International commercial law', 'Human rights in the information society'. Yves Poullet heads the CRID, since its creation in 1979. He conducts various research projects in the field of new technologies with a special emphasis on privacy issues, individual and public freedom in the Information Society and Internet Governance. He is legal experts near the UNESCO and the Council of Europe. During 12 years (1992–2004) he has been a member of the Belgian data Protection Authority. In addition, he was since its origin, member of Legal Advisory Board of European Commission and the president of the Task Force 'Electronic Democracy and Access to public records'. He has received the Franqui Chair in 2004.

He also chaired the Belgian Computer Association Association Belge de Droit de l'Informatique (ABDI). He is an active member of the editorial board of various famous law reviews. He is a founder of the European Telecommunication Forum, ECLIP and FIRILITE.

Charles Raab is a professor emeritus and honorary professorial fellow in the School of Social and Political Science at the University of Edinburgh, where he was a professor of government and is associated with the Institute for the Study of Science, Technology and Innovation (ISSTI). He has conducted research and published books and articles extensively in the field of information policy and regulation, with particular emphasis upon privacy and data protection, surveillance, the use and sharing of personal data in government, personal identity, and freedom of information. He has held visiting positions at Tilburg University (TILT), Queen's University, Kingston, Ontario, the Oxford Internet Institute, and the Hanse-Wissenschaftskolleg at Delmenhorst, Germany. He serves on the editorial or advisory boards of many academic journals, and on the advisory boards of

several research projects. He is a member of the Surveillance Studies Network, and participates in the Canadian-funded project on 'The New Transparency: Surveillance and Social Sorting' and in the European Union's COST Action on 'Living in Surveillance Societies' (LiSS). His consultancy work has included the European Commission, the United Kingdom Government, and the Scottish Government. He was the Specialist Adviser to the House of Lords Select Committee on the Constitution for their inquiry, *Surveillance: Citizens and the State*, 2nd Report, Session 2008–2009, HL 18.

Stefano Rodotà Professor of law, University of Roma 'La Sapienza'. Chair of the scientific Committee of the Agency for Fundamental Rights, European Union. Chair, Internet Governance Forum Italy. Former President of the Italian Data Protection Commission and of the European Group on Data Protection. Member of the Convention for the Charter of Fundamental Rights of the European Union. Visiting Fellow, All Souls College, Oxford. Visiting Professor, Stanford School of Law. Professeur à la Faculté de Droit, Paris 1, Panthéon-Sorbonne. Laurea honoris causa Université «Michel de Montaigne», Bordeaux. Former Member of the Italian and European Parliament, of the Parliamentary Assembly of the Council of Europe. Among his books: Tecnologie e diritti, Bologna, 1995; Tecnopolitica, Roma-Bari, 2004 (translated into French and Spanish); Intervista su privacy e libertà, Roma-Bari, 2005; La vita e le regole. Tra diritto e non diritto, Milano, 2006; Dal soggetto alla persona, Napoli, 2007.

Antoinette Rouvroy is FNRS (National Fund for Scientific Research) research associate and researcher at the Information Technology and Law Research Centre (CRID) of the University of Namur, Belgium. She is particularly interested in the mechanisms of mutual production between sciences and technologies and cultural, political, economic and legal frameworks. Her doctoral research at the European University Institute of Florence (Human Genes and Neoliberal Governance: A Foucauldian Critique. Abingdon and New-York, Routledge-Cavendish, 2008), looked at the knowledge–power relations in the post-genomic era. Her current interdisciplinary research interests revolve around the ethical, legal and political challenges raised by the new information, communication and surveillance technologies (biometrics, RFIDs, ubiquitous computing, ambient intelligence, persuasive technologies . . .) and their convergence.

Dag Wiese Schartum is a professor of law and chair of the Norwegian Research Center for Computers and Law (NRCCL) at the University of Oslo. Schartum's research interests comprise data protection, automated decision-making in government sector, access to government-held information and regulatory management. Dag Wiese Schartum has been member of several governmental expert committees and was, e.g., member of the committee drafting the Data Protection Act. In 2006 and 2008 the Ministry of Justice and Police engaged him and Lee A. Bygrave to evaluate and propose how the Norwegian Data Protection Act could be amended. List of books and articles by Schartum are available from http://www.schartum.no (cf. "bøker" and "artikler").

Ivan Szekely is an internationally known expert in the multidisciplinary fields of data protection and freedom of information. A long-time independent researcher, consultant and university lecturer, former chief counselor of the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, he is at present Counselor of the Open Society Archives at Central European University and associate professor at the Budapest University of Technology and Economics. He has conducted research in the areas of data protection, information privacy, access to public information and archivistics. He participated in founding several national and international organizations in the area of data protection and FOI, shaping their strategies and activities. As member of experts' teams, he contributed to the framing and drafting of legislation regarding openness and secrecy in several new European democracies. A university professor, regular conference lecturer and author of notable publications, Szekely is member of several international research groups, among others, the 'Broadening the Range Of Awareness in Data protection' (BROAD), the 'Ethical Issues of Emerging ICT Applications' (ETICA) projects and the 'Living in Surveillance Societies' (LiSS) COST Action of the European Union.

Pierre Trudel is a full professor at the Public Law Research Center of the Faculty of Law of the Université de Montréal. He holds the L.R. Wilson Chair on information technology law and electronic commerce. His research and teaching focus on civil law, legal theory, legal epistemology, civil rights, fundamental information rights, intellectual property and information, media and communication law. He is a co-author with France Abran and Lucie Guibault, of Droit de la radio et de la télévision (Radio and Television Law), 1991, and recipient of the Québec Bar Foundation Award in 1993 and the Walter Owen Award in 1994. He also published *La carte à mémoire: ses aspects juridiques et technologiques* (Smart Card, Legal and Technological Aspects, 1992) and *La preuve et la signature dans l'échange de documents informatisés* (Evidence and Signature in EDI, 1993), (The Electronic Superhighway—The Shape of Technology and Law to Come, 1995, *L'intérêt public en droit de la communication* (1996), *Droit du cyberespace* (Cyberspace law), (1997), Cyberspace and Electronic Commerce law: general principles and legal issues (June 1999) and "The Development of Canadian Law with Respect to E-Government" in J.E.J. Prins, Designing e-Government, Kluwer Law International, 2007. He is currently involved in research and teaching on legal aspects of cyberspace regulation and Media law.

Jane K. Winn is the Charles I. Stone Professor as well as a faculty director of the Law, Technology and Arts program at the University of Washington School of Law. She is a graduate of the University of London and Harvard University. She also serves on the faculty of the University of Melbourne Law School where she has taught post-graduate courses in law and technology since 2001. In 2008, she was a Fulbright Scholar in China where she studied the impact of globalization and innovation on law. She is a leading international authority on electronic commerce law and technological and governance issues surrounding information security, and

has widely published in law journals in the United States and Europe. Her current research interests include electronic commerce law developments in the United States, the European Union, and China. She is coauthor of *Law of Electronic Commerce* and the casebook *Electronic Commerce*.

Part I
Fundamental Concepts

Chapter 1
Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action

P. De Hert and S. Gutwirth

Although the 'formal' protection of the right to respect for private life, at least in areas covered by the first pillar, is in essence relatively satisfactory, there are concerns surrounding the weakening of the 'substantial' protection of that right.[1]

1.1 Formal or Political Constitutionalisation

1.1.1 The Underlying Interests of Data Protection

It is impossible to summarise data protection in two or three lines. Data protection is a catch-all term for a series of ideas with regard to the processing of personal data (see below). By applying these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc. In general, data protection does not have a prohibitive nature like criminal law. Data subjects do not own their data. In many cases, they cannot prevent the processing of their data. Under the current state of affairs, data controllers (actors who process personal data) have the right to process data pertaining to others. Hence, data protection is pragmatic; it assumes that private and public actors need to be able to use personal information because this is often necessary for societal reasons. Data protection regulation does not protect us from data processing but from unlawful and/or disproportionate data processing.

P. De Hert (✉)
Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel, *Tilburg Institute of Law and Technology* (TILT) at Tilburg University
e-mail: paul.de.hert@vub.ac.be

S. Gutwirth
Vrije Universiteit Brussel (VUB) and Erasmus Universiteit Rotterdam

[1] Report on the First Report on the Implementation of the Data Protection Directive 95/46/EC, Committee on the Citizens' Rights and Freedoms, Justice and Home Affairs, European Parliament, Session Document, 24 February 2004 (Final A5-0104/2004), p. 13 http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/ep_report_cappato_04_en.pdf

S. Gutwirth et al. (eds.), *Reinventing Data Protection?*

DOI 10.1007/978-1-4020-9498-9_1,

Data protection regulation's real objective is to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details.[2] This objective seems to be indebted to the central objective of the right of privacy, to protect against unjustified interferences in personal life. Many scholars therefore hold data protection and privacy to be interchangeable. Data protection is perceived as a late privacy spin-off. We will come back to the relationship between privacy and data protection below. What we would like to underline here is that data protection regulation does a lot more than echoing a privacy right with regard to personal data. It formulates the conditions under which processing is legitimate. This entails, among other things that 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. Data protection also prohibits certain processing of personal data, for instance 'sensitive data'.[3] A key principle to determining what is legitimate and what is prohibited is the purpose specification principle: data may only be processed when it is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Next to these guidelines on legitimate and unlawful processing, few specific subjective rights are granted to the data subject. These are *inter alia* the right to be properly informed, the right to have access to one's own personal data, the right to have data rectified the right to be protected against the use of automated profiling, the right to swift procedures in court, the right to assistance by Data Protection Authorities (DPAs) which are competent for a variety of tasks and enjoy broad discretionary powers (reporting, monitoring, complaints handling, rule development, enforcement), a right upon security measures to be implemented by 'controllers' and 'processors' and the right that only relevant data will be gathered and that they will not be disclosed except with consent of data subject or by authority of law.

We see data protection as a growing body of rules and principles that need to be taken into account by the legislator in drafting laws and by 'controllers' and 'processors of personal data'. This process is never over. New rules and principles are called for every time new challenges arise due to new (technological) developments. It is therefore not easy to define the underlying interest of data protection. Just as there are many visions of privacy in literature from narrow visions (*protection of the intimate sphere* proposed by inter alia Wacks, Inness),[4] older visions (*the*

---

[2] P.J. Hustinx, 'Data protection in the European Union', *Privacy & Informatie*, 2005, No. 2, (pp. 62–65), p. 62.

[3] Data protection law includes extra safeguards with regard to the processing of sensitive data or 'special categories of data', such as data on ethnicity, gender, sexual life, political opinions or the religion of the person. The special responsibility of the data processor towards sensitive data can be explained by the fact that the information at stake, for example medical data, belongs to the core of a person's private life. It is exactly this kind of information that individuals generally do not wish to disclose to others.

[4] Raymond Wacks, 'The Poverty of Privacy', *Law Quarterly Review*, 1980, vol. 96, p. 73 ff.; Julie C. Inness, *Privacy, Intimacy, and Isolation*, Oxford. University Press, 1992.

right to be let alone proposed by Warren & Brandeis or the dignity approach),[5] newer visions ('identity' as proposed by Hildebrandt)[6] over to broader visions (*privacy as freedom and informational self-determination* proposed by inter alia Westin and Gutwirth),[7] there are many possible 'readings' regarding the interests underlying data protection and their priority, ranging from autonomy, informational self-determination, balance of powers, informational division of powers, over integrity and dignity, to democracy and pluralism.[8]

1.1.2 Formal Constitutionalism and the History of Data Protection

The history of European data protection is a well-known example of legal creativity and perseverance of some of the visionary in the policy making world, realizing that the right to privacy in Article 8 of the European Convention for the protection of human rights and fundamental freedoms (ECHR), adopted in 1950, needed to be complemented to meet some of the challenges created by emerging technologies in the 1970s.[9] In the early 1970s the Council of Europe concluded that Article 8 ECHR suffered from number of limitations in the light of new developments, particularly in the area of information technology: the uncertain scope of private life, the emphasis on protection against interference by public authorities, and the insufficient response to the growing need for a positive and proactive approach, also in relation to other relevant organisations and interests.[10] As a consequence,

---

[5] Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy', *Harvard L. Rev*. 1890, pp. 195–215; Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' *N.Y.U. L. REV.*, 1964, Vol. 39, p. 962 ff.

[6] M. Hildebrandt, 'Privacy and Identity', in Claes, E., Duff, E., Gutwirth, S. (eds.), *Privacy and the Criminal Law*, Antwerp- Oxford: Intersentia 2006, pp. 43–58.

[7] F. Westin, *Privacy and Freedom*, Bodley Head, London, 1967; S. Gutwirth, *Privacy and the information age*, Lanham/Boulder/New York/Oxford, Rowman & Littlefield Publ., 2002, 146p.

[8] E. Brouwer, *Digital Borders and Real Rights.* Nijmegen, Wolf Legal Publishers, 2007, (501p.), p. 170–175; P. De Hert & S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, p. 61–104; L. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Deventer, Kluwer Law International, 2002, 448p.; L. Bygrave, 'Regulatory logic of data protection laws', February 2007, (2p.), p. 1 (via http://www.uio.no/studier/emner/jus/jus/JUR5630/v07/undervisningsmateriale/lecture5v07.doc). Cf. the contribution of Poullet and Rouvroy in this book.

[9] See in more detail: P. De Hert & S. Gutwirth, 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute for Prospective Technological Studies-Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, p. 125–127. See also Birte Siemen, *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot, 2006. 351 p. See on this excellent study the book review by Cornelia Riehle, *CML Rev. 2007*, pp. 1192–1193.

[10] P.J. Hustinx, *l.c.*, p. 62.