Innovation – The European Journal of Social Science Research
Vol. 23, No. 1, March 2010, 61–67

Routledge
Taylor & Francis Group

RESEARCH NOTE

Privacy, data protection and emerging sciences and technologies: towards a common framework

Michael Friedewald[a]*, David Wright[b], Serge Gutwirth[c] and Emilio Mordini[d]

[a]*Fraunhofer Institute for Systems and Innovation Research, Breslauer Straße 48, 76139 Karlsruhe, Germany;* [b]*Trilateral Research and Consulting, London, UK;* [c]*Research Group on Law Science Technology and Society, Vrije Universiteit Brussels, Belgium;* [d]*Center for Science, Society and Citizenship, Rome, Italy*

(*Received 29 January 2010; final version received 23 February 2010*)

Privacy is an important fundamental human right. It underpins human dignity and other values such as freedom of association and freedom of speech. However, privacy is being challenged in the networked society. The use of new technologies undermines this right because it facilitates the collection, storage, processing and combination of personal data by security agencies and businesses. This research note presents the background and agenda of the recently-commenced research project PRESCIENT, which aims at reconceptualizing the concept of privacy and developing means for the assessment of privacy impacts.

Keywords: privacy; data protection; impact assessment; ethics; policy-making

Introduction

Privacy is a multifaceted concept that is currently being challenged by many developments in science and technology. Some of the most prominent examples are identification technologies such as radio frequency identification (RFID), social network services such as Facebook and the creation of large bio banks.

Privacy is a moving target. It is evolving over time. People define it differently and value it differently. Moreover, privacy is often balanced against other values, such as the safety and security of society. Empirical research is needed to determine how people value privacy, however they define it, in order to understand how citizens understand the right to privacy and its value within the whole context of other fundamental rights.

Privacy can be viewed in various ways, e.g. as a right to confidentiality of communications, a right to be left alone, a right to control one's own life or a right to the protection of one's personal data. Privacy also describes an important aspect of one of the main, vital and constitutive dualities that shape human beings, i.e. the tension between individuals and the community. The PRESCIENT project, recently funded by the European Commission, aims to examine how new technologies impact on this complex concept and to identify privacy issues arising from different emerging technologies. The three-year project is premised on the need for a multidisciplinary analysis in order to appreciate the various philosophical, political,

*Corresponding author. Email: Michael.Friedewald@isi.fraunhofer.de

ISSN 1351-1610 print/ISSN 1469-8412 online
© 2010 Interdisciplinary Centre for Comparative Research in the Social Sciences and ICCR Foundation
DOI: 10.1080/13511611003791182
http://www.informaworld.com

legal, ethical and social meanings of the word "privacy" in the contemporary technological world.

The project also recognizes that privacy is a salient topic in technology policy-making and that there is a need for a new social dialogue on privacy rights that includes issues such as the new borders of the private domain, a new business ethics and a dialogue on the balance between civil and government rights. Proceeding from the privacy problems posed by new technologies, the project aims at establishing a new taxonomy of privacy problems to help policy-makers balance privacy against countervailing values, rights, obligations and interests.

Development from a legal perspective

Since the end of the nineteenth century, the concept of privacy has progressively become a legal term. Today, privacy is recognized as a right in different major international legal instruments. The Universal Declaration of Human Rights (UDHR), establishes it in Article 12, which states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations 1948). The International Covenant on Civil and Political Rights includes a right to privacy in its Article 17, which is almost identical to Article 12 of the UDHR (United Nations 1966). The European Convention of Human Rights (ECHR; Council of Europe 1950/1998)[1] recognizes the right to privacy in its Article 8, the scope of which seeks to protect four different areas of personal autonomy, which are not mutually exclusive: private life, family life, the home and one's correspondence. The Charter of Fundamental Rights of the European Union explicitly recognizes the right to privacy in Article 7 and uses the same wording as Article 8 of the ECHR.

The right to privacy protects the fundamental political values of democratic constitutional states, as it guarantees individuals their freedom of self-determination, their right to be different, their autonomy to engage in relationships, their freedom of choice and their autonomy as regards their sexuality, health, social behavior, etc. It guarantees each person's uniqueness, including alternative behavior and the resistance to power at a time when it clashes with other interests (De Hert and Gutwirth 2006, p. 70). By default, privacy prohibits interference of the state and private actors in the individual's autonomy: it shields the individual from intrusions. The scope and reach of privacy are un(der)determined: it is up to judges to decide when privacy interests are at stake and when their protection can rightfully be invoked. Legislators can also intervene to protect specific privacy interests, for example, through enacting laws on professional secrets, the secrecy of communications or the inviolability of the home.

Article 8 of the Charter of Fundamental Rights of the European Union recognizes the fundamental right to the protection of personal data. The introduction of this article in the 2000 Charter has a long history. It was inspired by the guidelines of the OECD (1980) governing the protection of privacy and transborder flows of personal data, the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of the Council of Europe (1981) and by EU legislation, notably the EU Data Protection Directive (European Community 1995).

Towards a new privacy framework

Data protection is both broader and more specific than the right to privacy. The relationship between these concepts is certainly something that needs to be addressed for a reconceptualization of privacy. Data protection is broader because it not only aims at making the protection of privacy concrete, but it also tends to protect other rights and interests such as freedom of expression, freedom of religion and conscience, the free flow of information and the principle of non-discrimination. It is more specific, since it applies every time personal data are processed. The application of data protection rules does not require an answer to the question of a violation of privacy: data protection applies when the conditions stipulated by legislation are fulfilled. Furthermore, data protection rules are not prohibitive by default; they channel and control the way personal data are processed. Such data can only be legitimately processed provided some conditions pertaining to the transparency of the processing and the accountability of the data controller are met.

Yet, with the "technology revolution", the concept of privacy has embarked on a new journey, beyond the merely legal sphere, which is probably leading privacy back to its original roots, the relationship between the citizen and the "polis". We are facing new contexts (think, for example, of the so-called PAN, personal area network, which describes a technology that could enable wearable computer devices to communicate with other nearby computers and exchange data) and new concepts (like, for example, the idea of genomic and proteomic information), not to mention issues raised by technologies such as biometrics, RFID, smart surveillance systems, body implants, nano devices and the like, all of which will be the subject of case studies in the PRESCIENT project.

New technologies have some specific features that make them quite different from traditional industrial technologies. In comparison with the technologies that drove the industrial revolution – which were complex, based on collective action, social infrastructure and technical know-how – emerging technologies are lighter. They are decentered, dispersed and disseminated, and their control and use are largely in the hands of individuals, citizens' groups and small enterprises. They are network technologies (Castells 1996). In addition, new technologies help reduce the complexity of human (social, biological, political, etc.) interactions and allow the individual to distance himself from his observation. As Paul Virilio (1995) has emphasized, new technologies always bring about even more and even faster new technologies. Emerging technologies also imply a change in the relationship between science and politics. Over the last few decades, the representation of science has changed so much that some people might say that "doing science is another way of doing politics". Indeed, the postmodern technological system is embedded in politics. Researchers are coming under increasing pressure to demonstrate the policy relevance of their findings and to deliver tangible results. In turn, policy-makers are facing increasing pressure to justify their choices of technology to be developed and the socio-economic goals to be pursued. As emerging technologies often challenge basic moral assumptions, they provoke a crisis directly or indirectly, or at least a basic uncertainty with regard to moral standards that are either sanctioned by law or remain tacit presuppositions. This results in a growing gap between citizens, technology and politics, notably when the individual's private sphere conflicts with the notion of common good.

The PRESCIENT project

The European Commission (EC) is now recognizing the need to reconceptualize privacy, to develop suitable methods in order to assess the impacts that emerging technologies have and to consider privacy a central element in the global governance of science and technology. To this end, PRESCIENT (Privacy and Emerging Sciences and Technologies: Towards a Common Framework)[2] aims to establish a new framework for privacy and ethical considerations arising from emerging technologies (see Box 1). The project, which began in January 2010, will pursue this by addressing four main issues:

(1) *The legal, social, economic and ethical dimensions of privacy.* Since the late nineteenth century, privacy has been considered mainly in legal terms. PRESCIENT will review and analyze the social, economic and ethical dimensions of privacy as well as, and in particular, how these different approaches affect one another and what bridges can be built between these different approaches.

Box 1. Project: Privacy and Emerging Sciences and Technologies (PRESCIENT).

- Funded in the "Science in Society" programme under the EU's Seventh Framework Programme (small or medium-scale focused research project)
- Partners: Fraunhofer Institute for Systems and Innovation Research, Germany (coordinator); Trilateral Research and Consulting LLP, UK; Center for Science, Society and Citizenship, Italy; Vrije Universiteit Brussels, Research Group on Law Science Technologyand Society, Belgium
- Project duration: January 2010 to December 2012 (36 months)

The PRESCIENT project unfolds in four stages.
The first stage is a *state-of-the-art analysis* of privacy and data protection as conceptualized from legal, social, economic and ethical perspectives.
The second stage consists of *case studies* in which the partners will identify the privacy, data protection and ethical issues arising from five different emerging technologies and their applications, including identification and localization technologies, smart surveillance technologies, biometrics, on-the-spot DNA sequencing and technologies for human enhancement.
The third stage focuses on *citizens.* The partners will analyze various existing surveys to assess citizens' concerns and awareness of the ways in which their data are collected, stored and used and their anxieties about new technologies and how these worries have changed over time.
The fourth and final stage focuses on developing a *new framework for privacy and ethical impact assessment*. The partners will develop scenarios as an element in this new framework, based on an integration of the results of this study and on privacy impact assessment guidelines.

(2) *The privacy and ethical implications of emerging technologies.* PRESCIENT intends to carry out case studies of five different emerging technologies to determine whether there are privacy problems posed by them that do not easily fall within a taxonomy of privacy problems, such as the one suggested by Solove (2008). These five cases include (1) localization and identification technologies, (2) smart surveillance, (3) biometrics, (4) on-the-spot DNA analysis and (5) technologies for human enhancement. The problem with framing privacy solely in individualistic terms is that privacy becomes undervalued. The interests aligned against privacy – for example, efficient consumer transactions, free speech or security – are often defined in terms of their larger social value. In this way, protecting the privacy of the individual seems extravagant when weighed against the interests of society as a whole. Ethical issues will also need to be addressed, especially as they come in increasing numbers and are often "packaged" in terms of complex technology. Considerable effort will be required to comprehend such ethical issues as well as to formulate and justify good ethical policies. People who both understand the technologies and are knowledgeable about ethics are in short supply, just as the need for them is expanding (Moor 2005, p. 118).

(3) *Privacy impact assessment* (PIA). In Europe, policy-makers have been considering the adequacy of data protection legislation, the powers accorded national data protection authorities and the tension between facilitating trade and transborder data flows, whilst ensuring personal data are protected and accessible and not abused once they leave European jurisdiction.[3] There has been a primary focus on legislative considerations. At the same time, the EC and others have been concerned about the advent of new technologies and how their possible privacy impacts can be addressed. The EC's RFID consultation, in some ways, can be considered a ground-breaking initiative in the sense that the EC has initiated a consultation with stakeholders on the introduction and deployment of a new technology, something that has not really happened before. It also recommended the use of privacy impact assessments in new RFID applications. Although PIAs have been around for more than a decade in a few other countries, notably Australia, Canada, Hong Kong, New Zealand and the United States, they have only recently been introduced (by the UK Information Commissioner's Office) as a tool in Europe (Bennett et al. 2007). Use of PIAs is likely to grow in the coming years. The PRESCIENT project will make the case for more extensive use of PIAs modified to take into account ethical considerations. PIAs used in tandem with ethical impact assessments could do much to come to terms with stakeholder apprehensions and, more specifically, a lack of public and stakeholder awareness of new technologies and their ethical implications before the technologies are widely deployed.

(4) *Privacy policies.* Technology, particularly revolutionary technology, generates many ethical problems. Sometimes the problems can be treated easily under extant ethical policies, but at other times – because new technology allows us to perform activities in new ways – situations may arise in which we do not have adequate policies in place to guide us. Sometimes we can anticipate that the use of the technology will have clearly undesirable consequences. As much as possible, we need to anticipate these and establish

> policies that will minimize the adverse effects of the new technology (Moor 2005, p. 115).

Understanding and taking into account the role of stakeholders, including the public, is important because it colours our (social) notions of privacy and how we assess the impacts of new and emerging technologies. More importantly, we need to take these views into account as a matter of social equity: new technologies and the issues they raise will affect the public, so the public must be consulted and given the opportunity to participate in policy-making. The privacy and ethical impact assessment framework to be developed by the PRESCIENT partners will be a way of unearthing and assessing ethical problems associated with a new technology and involving stakeholders in the process. A final task of the project will be to formulate recommendations with regard to ethical approaches to the development of new technologies and to the weighing of privacy and data protection issues against other values.

Acknowledgements

This work was carried out in the EU-funded FP7 project PRESCIENT: Privacy and Emerging Sciences and Technologies (SIS-CT-2009-244779).

Notes

1. Note that the EU must generally respect fundamental rights as guaranteed by the ECHR by virtue of Article 6(2) of the Treaty of the European Union.
2. http://www.prescient-project.eu/.
3. The Article 29 Data Protection Working Party has raised these and other issues in its recent paper. See Article 29 Data Protection Working Party and Working Party on Police and Justice. 2010. *The future of privacy: joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Working Paper 168. Brussels. Available from: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

References

Bennett, C., Bayley, R., Clarke, R. and Charlesworth, A., 2007. *Privacy impact assessments: international study of their application and effects report for the Information Commissioner's Office*. London: Linden Consulting. Available from: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

Castells, M., 1996. *The rise of the network society. Vol. 1: the information age: economy, society and culture*. Oxford: Blackwell.

Council of Europe. 1981. *Convention for the protection of individuals with regard to the automatic processing of personal data*, ETS 108. Available from: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Council of Europe. 1950/1998. *European convention for the protection of human rights and fundamental freedoms as amended by Protocol No. 11*. ETS No. 155. Available from: http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

De Hert, P. and Gutwirth, S., 2006. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. *In*: E. Claes, A. Duff, and S. Gutwirth, eds. *Privacy and the criminal law*. Antwerp: Intersentia, 61–104.

European Community. 1995. 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 on the free movement of such data. OJ No. 281, 23.11.95, pp. 31–50.

Moor, J.H., 2005. Why we need better ethics for emerging technologies. *Ethics and information technology*, 7, 111–120.
OECD. 1980. *Guidelines governing the protection of privacy and transborder data flows of personal data*. Paris: OECD.
Solove, D.J., 2008. *Understanding privacy*. Cambridge, MA: Harvard University Press.
United Nations. 1948. *Universal declaration of human rights*. GA res. 217A (III), UN Doc. A/810, pp. 71–79.
United Nations. 1966. *International covenant on civil and political rights*. GA res. 2200A (XXI), pp. 49–60.
Virilio, P., 1995. *The art of the motor*. Minneapolis, MN: University of Minnesota Press.

Copyright of Innovation: The European Journal of Social Sciences is the property of Routledge and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.