EDITORIAL

Technology and privacy

This text is published as: Michael Friedewald & Ronald J. Pohoryles (2013): Technology and privacy, Innovation: The European Journal of Social Science Research, 26:1-2, pp. 1-6. http://dx.doi.org/10.1080/13511610.2013.768011

Privacy and data protection are recognized as fundamental human rights.[1] They underpin human dignity and other values such as freedom of association and freedom of speech. Indeed they have become two of the most important human rights of the modern age. However, new technologies undermine individual rights because they facilitate the collection, storage, processing and combination of personal data for the use not only of government agencies, but also of businesses.

Technology and privacy are two intertwined notions that must be jointly analyzed and faced. Technology is a social practice that embodies the capacity of societies to transform themselves by creating the possibility to generate and manipulate not only physical objects, but also symbols, cultural forms and social relations. In turn, privacy describes a vital and complex aspect of these social relations. Thus technology influences peoples understanding of privacy, and peoples understanding of privacy is a key factor in defining the direction of technological development. Either policy-making takes into account this rich and nuanced interplay between technology and privacy or we run the risk of failing to govern the current, concomitant technology and privacy revolutions.

Modern technologies have not "created" challenges to privacy: if we take the example of online social networks, even without them, communication within the framework of "social networks" takes place. Information shared with friends or colleagues in the traditional way might be "leaked" by one of these and give rise to gossip, rumors, etc. However, the sheer quantity involved in online social networks leads to new qualities: while traditional information channels are limited to a normally known group of people and, hence, the "leak" can be traced, the worldwide net is accessible to everybody who has a certain level of technical knowledge. The information, even if restricted to a small group of users, can be used by others, be it for commercial ends, political reasons or personal malicious purposes. The use of modern technology requires personal responsibility, but this can only be based upon ICT literacy.

Hence, innovation in the field of privacy, especially with regard to new technologies, also requires innovative legal and political frameworks that can ensure that the implications of ICT are not only known, but also adequately governed. This task is often threatened by the understanding of privacy as such, perceptible through the many ways in which privacy is addressed and analyzed.

A good example here is the use of mobile communication devices. The recent European Directive on Data Retention has made people aware of the conflict between the comfort of using such devices and the threat to their privacy.[2] However, there is little awareness that the data can be used for other purposes than "just" ensuring security, as this directive alarmingly makes clear. The data can be used for purposes such as the analysis of traffic flows, tourism statistics, regional statistics, etc. If the data, for instance, are gained through the statistics of mobile com- munication operators, which store the data anyway, the danger for privacy becomes obvious. After all, these data are not anonymized and can be misused for all kinds of private and public purposes. The key concept of privacy has generated four main ideas.

Privacy as a multifaceted concept

Privacy is not only respect for confidentiality, although it implies this. Privacy is not only the right to be left alone, although it includes this. Privacy is not only the right to control ones own life, although it entails this. Nor is privacy only data protection, although it also concerns this. Privacy is all these things together, and more, because privacy is the word we use to describe an important aspect of one of the main, vital and constitutive polarities that shape human beings, that is, the tension between the individual and the community. How do new technologies impact on this complex and rich concept? What are the privacy issues arising from different emerging technologies? Multidisciplinary analysis is needed in order to appreciate the various philosophical, political, legal, ethical and social meanings of the word "privacy" in the contemporary technological world.

Data protection is both wider and more specific than the right to privacy. The relationship between these concepts is certainly something that needs to be addressed in order to arrive at a new concept of privacy. Data protection goes wider because it not only aims to ensure the protection of personal data, but also tends to protect other related rights and interests such as the freedom of expression, and the freedom of thought, conscience and religion. At the same time it also enables the free flow of information in a non-discriminatory way. Yet data protection is also more specific, because it only applies in situations in which personal data are processed. The application of data protection rules does not require an answer to the question of privacy violation: data protection applies when the legal conditions are fulfilled.

Furthermore, data protection rules are not a prohibition by default; they channel and control the way personal data is processed. Such data can only be legitimately processed if certain conditions pertaining to the transparency of the processing and the accountability of the data controller are met. Privacy, however, sets *exclusionary* limits that shield the individual against state (and other) powers, thus warranting a certain level of *opacity* of the citizen.

Privacy as a moving target

The concept of privacy has evolved with time. People also define and value it differently depending on context. Moreover, privacy is often balanced against other values, such as societys safety and security. There is little empirical data on citizens perceptions of various aspects of privacy, especially how it relates to actual behavior. Empirical research on how people value privacy, however they define it, is thus needed in order to understand how real citizens understand the right to privacy and its value within a social model and system of fundamental rights.

Yet with the "technology revolution" the notion of privacy has started a new journey — beyond the legal sphere — which is probably leading privacy back to its original roots, the relation between the citizen and the "polis". We are immersed in new contexts (think, for instance, of ICT (information and communication technologies) implants, with which it becomes possible for a technologically "enhanced" body to communicate with nearby computers and exchange data) and new concepts (for example, the idea of genomic and proteomic information), not to mention issues raised by technologies such as biometrics, smart surveillance systems, body implants and neurotechnology, among others.

These new technologies have specific features that make them quite different from traditional industrial technologies. Compared 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 decentralized, dispersed and disseminated, and their control and use are largely in the hands of the individuals, citizen groups and small enterprises. Also the substance and aim of their operation is different — manipulation of information as substance of human interaction as opposed to production of solid objects — therefore the characteristics of cause and effect are based on a different set of principles.

Privacy as a salient topic in technology policy-making

There is a need for a new social debate on privacy rights that includes issues such as the new boundaries of the private domain, new business ethics and the balance between civil rights and governmental spheres of competence. This is probably something governments need to consider. It is necessary to produce a new taxonomy of privacy problems — including all those posed by new technologies — that could help policy-makers and decision-takers to better weigh up privacy against counter-vailing values, rights, obligations and interests. Consequently this implies a change in the relationship between science and politics.

The post-modern technological system is highly embedded in politics. Researchers are under increasing pressure to demonstrate the policy relevance of their findings and to deliver tangible results. In turn, policy-makers are under pressure to justify their choices of technologies to be developed and socio-economic goals to be achieved.

Because they challenge assumptions at the root of our current morals, emerging technologies are provoking a crisis — or at least a basic uncertainty with regard to moral standards — that is either sanctioned by law or remains at the level of tacit presuppositions. This leads to a growing gap between citizens, technology and politics, most evident when the individuals private sphere conflicts with the notion of common good.

Privacy as an issue of personal responsibility

Privacy is both an issue of political regulation, and one of personal concern, in the sense that it concerns the balance between public/personal security and liberty. The difficulty, when it comes to the introduction of new technologies, is the way in which these are used, perceived and handled, not only by state actors in order to ensure security in the public space, but also by individual users in their own, increasingly virtual space. Major concerns have arisen following the widespread use of "social networks": users tend to underestimate the dangers of publishing private matters and, hence, tend to underestimate the importance of carefully choosing what they want to keep private. Once published in virtual space the data never disappear without a trace. Even if the information is more often than not only accessible to a specified group of recipients, it can be made public by users who might be unaware of the necessity to keep private things private, or who are malicious enough to hack those networks and use the data for their own purposes. The internet is in fact not a private sphere at all.

Another telling example of the Janus-faced characteristics of modern ICT is the example of smart grids: smart grid technologies enable people (1) to understand how their household uses energy, (2) to control expenditure of electricity, (3) to experience fewer and shorter power outages, and (4) to control energy devices in households. In this respect these technologies empower customers by providing them in a timely way with relevant information on their energy use, and with an overarching regulatory framework for reducing costs and their carbon footprint. This might, however, resonate as a ”sanctity of the home” issue, as personal details of daily life and individual habits should not be accessible. Additionally, very important concerns are that the privacy implications of smart grids are not yet fully understood and that formal privacy policies, procedures or standards are still insufficient on the side of the entities that are involved in the development of smart grids. Against this background, privacy issues need to be the utmost concern when analyzing the behavior of customers, as well as in attempts to increase their participation in active demand and to empower end users.

The contributions

This thematic issue contains 11 articles that focus on three different aspects of the relationship between technology and privacy. The four articles in the first part deal with aspects of privacy raised by specific new technologies.

One of these is cloud computing, that is, computer systems where information and/or applications are stored online, allowing access by the user over the Internet; recently cloud computing has raised many security and privacy concerns. In their article, Charlesworth and Pearson deal with the challenges presented by cloud computing for data protection. They see a general deficit in the current approach to regulation and advocate the principle of accountability in the governance of new technologies. They examine both procedural and technical solutions to demonstrate that accountability is a solution to juridical privacy and security risks.

In the next article in this part of the journal, Pocs deals with the question of how to ensure that respect for fundamental rights is taken into account in the design of future biometric systems for crime prevention. For this purpose Pocs suggests how technology design could render the violation of a legal norm impossible.

The third contribution is Mllers and Hlterleins analysis of the public discourse on surveillance technologies and privacy. Drawing on the case of ”smart” closed-circuit television in Germany, they show how privacy concerns are socially constructed and change over time, before raising questions for further investigation.

Finally, the research note by Bhle et al. deals with the optimization of human-computer interaction through biocybernetic adaptation. This approach increasingly uses body-related data to detect internal human states (emotion, feelings, possibly even intentions and thoughts) that can be used to control technical systems. It thus raises fundamental data protection and privacy questions. The authors outline possible opportunities, discuss privacy challenges and potential regulatory actions to be taken.

The articles in the second part focus on the important questions surrounding citizens perceptions of privacy, and challenges to privacy arising from new technologies and their application.

In their contribution Regan et al. investigate whether there are any differences in attitudes towards ICT and information privacy among members of different generations. They find that the empirical basis is rather too small to draw some general conclusions, but discover some interesting patterns.

In the following paper, Budak et al. empirically investigate attitudes towards privacy, data protection, surveillance and security in Croatia. They reach the conclusion that citizens can be divided into three types related to demographic groups in society: "pro-surveillance" oriented citizens; citizens concerned about being surveilled; and citizens concerned about privacy and data protection.

Van Lieshout et al. finally consider the relationship between privacy and security and, in particular, the traditional "trade-off" paradigm that used to be very popular among policy-makers and the surveillance industry. By refusing this simplistic model, they explore whether and how, in a democracy, one can reconcile the trend towards increasing security with the fundamental right to privacy. They present a research agenda for exploring the "real" relationship between privacy and security attitudes in a multidisciplinary and transdisciplinary way.

Finally, the third part covers legal aspects of privacy and data protection — including the consideration of new instruments for their protection. Although we initially stressed that privacy and data protection are two separate concepts that should not be understood as synonymous, data protection remains an important field when it comes to government regulation of emerging sciences and technologies. In that respect the European Commissions initiative for a new data protection regulation is probably the most important development in recent years.

De Hert et al. present an initial analysis of the proposed regulation, highlighting the treatment of basic data protection principles and elements and elucidating their merits and shortcomings.

Agustina and Coudert analyze the expanding use of legitimate covert CCTV in the workplace in Spain. The authors focus on the legal reasons that support court decisions from 2000 to the present and add some criminological and ethical perspectives to better comprehend not only its legal rationale, but also some other collateral effects that employers should take into account in implementing covert surveillance. The results of the study guide the development of a more detailed rationale for improving legal and decision-making analyses in this field.

Wadhwa and Rodriguess article focuses on privacy impact assessments (PIA). These have been intensively discussed in recent years and have been taken up in

Article 33 of the proposed European regulation on data protection, while Article 23 more generally sets out the obligation to follow the principle of data protection by design. Based on good practices, it outlines and evaluates criteria that could be used to turn PIA into an effective instrument taking into account the interests of all stakeholders.

Hornung points out in his article why attempts to introduce privacy by design and privacy enhancing technologies (PETs) have been notoriously unsuccessful in the past few years. He emphasizes that the current reform of data protection law is a unique opportunity to implement at least basic instruments to supplement and foster the development and introduction of privacy by design and PETs.

Acknowledgement

This special thematic issue is a joint initiative of the EU projects PRACTIS[3] and PRESCIENT[4]. PRACTIS analyzes the potential impact of emerging technologies and their convergence on the fundamental individual and structural values in which the European legal right to privacy is rooted, as well as on societal perceptions and conceptions of privacy. PRESCIENT aims to contribute to the development of new instruments for the governance of science and technology, in particular, privacy and ethical impact assessments. PRACTIS as well as PRESCIENT are funded through the Seventh Framework Programme for Research in the area of "Science in Society".

Michael Friedewald
Co-ordinator PRESCIENT; Fraunhofer ISI
Ronald J. Pohoryles
Editor, Innovation; Partner, PRACTIS

Notes

[1] Although privacy and data protection are often used synonymously they are listed as separate rights in the European Charter of Human Rights (Articles 7 and 8 ECHR).

[2] In fact there are attempts to top up this Directive through a European citizen initiative. The Commission promised to evaluate the Directive and to re-consider it after two years. However, the report was not delivered last autumn when it was due.

[3] PRACTIS stands for ”Privacy — Appraising Challenges to Technology and Ethics”; see http://www.practis.org

[4] PRESCIENT stands for ”Privacy and Emerging Sciences and Technologies: Towards a common framework for privacy and ethical assessment”; see http://prescient-project.eu