Future-Proofing Privacy

Surveillance & Society

Debate

Future-Proofing Privacy: Time For An Ethical Introspection?

Judith Rauhofer

University of Edinburgh, Scotland. judith.rauhofer@ed.ac.uk

1. Where Are We?

When trying to establish whether privacy is dead or whether it is merely evolving, we may very well be asking the wrong question. While there is considerable evidence that the concept of privacy is undergoing a sea change in the eyes of both individuals and policy makers, it could be argued that this is merely an expression of a much more fundamental issue that underpins the technological, political and economic changes we have witnessed over the past decade.

It is true that anecdotal evidence suggests that individuals, both as citizens and consumers, no longer value their privacy the way they once did. Many claim that this is true in particular for younger people who seem increasingly comfortable with sharing even intimate details about themselves and their life with others, including a much wider range of "others" than their parents' generation would have done.[1] Much of this is attributed to the evolution of the "participatory culture" (Jenkins et al. 2006) that has developed online and that has shifted social interaction, as well as the expression of one's creativity to mediated spaces that allow for maximum interaction, but that also require a much higher level of individual exposure not only to the other participants in those spaces but to the intermediary.

Nevertheless, successive studies have shown that the wish for control over one's own information remains high with, for example, 78 per cent of respondents to a 2011 EU survey on privacy believing that their specific approval should be required before any kind of information about them is collected and processed (Eurobarometer 359, 2011). While awareness of potential intrusions may be lower than it once was (possibly due to the way in which many online services manage to create an atmosphere of selectiveness and intimacy where in practice there is none), it is increasingly clear that a general feeling of unease over unauthorized access to personal information prevails and that a sense of encroachment in cases where contextual boundaries of information control are breached remains (Nissenbaum 2010). Thus, teenagers who are happy to share with their peers details of their daily experiences, thoughts, emotions and social interactions will often go to extraordinary length to prevent their parents, teachers or others in authority over them from accessing those spaces they consider to be private (boyd and Marwick 2011). Similarly, the outrage at perceived violations of those spaces is real, as is the lack of trust that results from experiences of repeated intrusions and the unexpected shifting of boundaries, in particular by those providing those spaces or those who provide access to them.[2] In the EU, almost two thirds of consumers do not trust their telephone, mobile or internet access providers or providers of online services (search,

[1] See, however, boyd and Marwick (2011) for a critique of this assumption.
[2] For one recent example, see Vijayan (2012).

Rauhofer, J. 2012. Future-Proofing Privacy: Time For An Ethical Introspection? *Surveillance & Society* 10(3/4): 356-361. http://www.surveillance-and-society.org | ISSN: 1477-7487

social networking, etc.) to protect their personal information. In historically privacy-conscious Germany, the numbers are even higher (between 74 and 78 per cent) (Eurobarometer 359, 2011).

The reason why those consumers continue to provide their personal information to providers they do not seem to trust can arguably be found in the realization that, in order to be part of this new participatory culture, the disclosure of personal data has become inevitable, a take-it-or-leave-it offer on the part of providers who turn personal data into a new currency used to pay for many of the "free services" they offer (Eurobarometer 359, 2011). This approach sets people's desire to protect their personal information against their materialistic and social wants and thus effectively re-defines personal data as a freely tradable commodity.

At policy level, individuals' apparent acceptance of this commercial privacy trade-off has enabled a line of argument to develop that claims that no new regulation of personal data processing is required (and that, indeed, the existing rules should be relaxed) precisely because there is no obvious demand for such regulation (Johnson 2010 and Spiegel Online 2012). In the ongoing conflict between the individual's right to privacy and the commercial need for the free flow of personal data as an ever more important resource in the modern information society, this increasingly results in an emphasis of the economic importance of personal information, which is classified not merely as a business interest but as a common societal good (Reding 2012). At a time of global recession, the economic imperative has therefore joined "national security" as the public policy objective of choice to which individuals' privacy is expected to take a backseat.

However, this view ignores the possibility that much of consumer inertia in this area could be attributed to a general sense of powerlessness within populations where individuals, particularly in the online environment, uncritically accept privacy statements that authorize wide-ranging uses of personal information, often without reading them, not because they are not concerned about their data but because they know that, in reality, their choice is between accessing online services on the providers' terms or not at all (Edwards and Brown 2009). The transparency approach, originally designed to provide consumers with agency in their dealings with commercial partners, could therefore be said to have spectacularly failed to enable consumers to maintain any kind of control over their personal information that would still allow them equal participation in social and economic life in the 21st century.

More importantly, however, proponents of a more relaxed regulatory approach to the protection of personal data also wilfully ignore the traditional historical objectives for establishing a right to privacy, particularly within the continental European fundamental rights tradition. This tradition has never viewed privacy merely as an individual right, but as a societal or common value that must be upheld in order to protect "democratic substance" (Simitis 1984). Within this paradigm, there is no clear binary conflict between the right to privacy on the one hand and economic or security interests on the other. Rather, it views privacy as an essential instrument designed to assist in maintaining the delicate balance of power between individuals, commercial entities and public bodies that our democratic constitutional systems were set up to create and uphold. A need for privacy will therefore not solely show up in the "consumer" column of the societal ledger, but also in that column which includes the measures that protect the constitutional structure. A shift of power in one direction or the other is likely ultimately to not only affect individuals' (commercial) rights and freedoms, but also the foundations of democratic government itself. This has never been more clearly recognized than in the 1984 *Census* decision of the German Constitutional Court in which it accorded German citizens a right to informational self-determination (German Constitutional Court 1984). This right guarantees those citizens' ability to retire to an unobserved private sphere where they can process information and develop ideas and opinions without being subjected to undue influence by public or private entities that may, in other spaces, have power over them. It was therefore seen as an essential pre-requisite for the active participation of the citizenry in political life.

Viewed in this way, it is easy to see that contemporary arguments which advocate a concept of privacy as a more proprietary right, and which bestow on individuals the power to freely trade (or not) in their personal information, largely and purposefully ignore the much wider objective that historically informed the fundamental right to privacy and data protection.

2. What should the future look like?

With this in mind, the question arises whether we can really limit regulatory interventions to those that are mandated by "the reasonable expectation of privacy" of the average consumer. All too often this approach seems to weigh the balance in favour of the interests of commercial providers and law enforcement agencies, who will inevitably proceed to engage privacy advocates in lengthy and often fruitless discussions about what is "reasonable" in a given situation. As a general rule these discussions do little more than distract from the underlying tensions that must be resolved (the recent discussion that surrounds the new DNT standard is a point in case here), while adding almost nothing to the development of an appropriate privacy standard.

Instead of engaging in these discussions, stakeholders should seek to answer some of the more basic questions that underpin the fundamental rights edifice, namely, what kind of society do we want to live in and what kind of sacrifices (economic, political and technical) are we prepared to make for establishing that society?

To fulfil the right to privacy's original intention and promise would require us to take account not only of the short-term costs and benefits of an open exchange of personal information, but also the long-term risks we may encounter and the harms we may suffer—both as individuals and as citizens—if we continue to apply a relatively undiluted *caveat emptor* principle with regard to the collection and use of our personal information. A shift in emphasis from an instant gratification society to one that properly assesses and addresses long-term risk on the basis of ethical considerations is likely needed, not only with regard to environmental and climate concerns and economical and financial management, but also in the area of information rights. From Big Oil and Big Money to Big Data, the underlying questions remain the same, as do the political power structures within which those questions must be addressed.

Substantively, this may mean that privacy rights must be afforded greater weight when being balanced against competing interests, including economic and national security interests. In particular, we need to stress and acknowledge that those interests are not binaries in a zero sum game, but that instead an increase in privacy can result in increased economic success and improved security. Economically speaking, privacy-friendly business models, particularly online, may help establish and maintain users' trust in online services, which they may otherwise choose not to use in order to protect themselves. In the future, this is likely to be increasingly important particularly for those types of services that rely on being able to process large amounts of personal data (for example, social networking services and cloud computing services). Although social networking services have seen exponential increases in their user base since their inception, that growth has recently slowed as those services' ever more permissive approach to their users' privacy has hit the headlines.

As already explained above, in terms of national security it could be argued that this should be viewed in a wider sense than merely the defence of a nation against an external or internal enemy. In a democratic state based on the rule of law, attention should also be paid to any threat that is posed to a nation's wellbeing through the corruption of its constitutional institutions and tenets. Shifts in the balance of power between those institutions, business and citizens, which may easily arise from an "information imbalance", where one actor is able to exercise control over another based at least partly on what they know about them, are likely to reverberate throughout society, possibly to the point where the original constitutional settlement is put at risk. Protecting its citizens' right to privacy is likely to go some way

towards ensuring an appropriate "information balance" and thus those citizens' continued participation in the defence of those tenets and institutions. A lack of privacy protection, on the other hand, is likely to facilitate a division of society into privacy haves and have-nots, resulting in the likely disengagement of at least part of the population from the democratic process. A stronger global consensus on the need for enhanced privacy protection is therefore imperative, as a "race to the bottom" in which each country argues for a further watering down of privacy standards, ostensibly in order to provide its business community with a short-term competitive advantage (in this context, parallels may again be drawn between the data protection and financial and environmental regulation), risks much greater harm further down the line.

3. And what is the best means of acquiring that future?

In order to achieve this aim, we will have to ensure that the existing defensive discourse around data protection is replaced with a positive agenda for privacy. In the words of Nigel Shadbolt, Professor of Computer Science at the University of Southampton, we need a Warnock-style enquiry into the moral, not just the legal, framework that should govern our use of personal information (Rooney 2012). The Warnock Commission, which was established in the UK in 1984, inquired into the societal risks and benefits of human fertilisation and embryology. In the introduction to its report, the Commission describes its task as examining the "ethical implications of new developments in the field" directing its attention not just "to future practice and possible legislation, but to the principles on which such practices and such legislation would rest" (Department of Health and Social Security 1984). We are now at a point where we need a similar ethical enquiry into the kind of personal data processing that we, as a society, believe should be permitted, including types of data to be used, and the purposes for which they should be processed. Within such a context, we must distinguish clearly between those processing activities that are both individually and socially useful and those that are likely to pose a long-term threat to our societies.

Countries where strong privacy protection exists (like most of the EU member states) should resist external pressures to relax their regulatory requirements, and transfers of data to countries without appropriate privacy standards should be restricted much in the same way, as is the case under the current EU data protection framework, until binding international standards based on such an ethical enquiry can be agreed.

To prevent any use or exploitation of personal data that is not authorized by the individual to whom it relates, or that is not otherwise justified by internationally agreed public policy objectives, increased emphasis should be placed on strategies to achieve data minimization. This would most likely require a change in the mind-set of many designers and developers from an unfettered open data approach to a more socially responsible culture of innovation. While the former makes almost no distinction between the processing of personal and other information, thus viewing a technology's use of personal data as a non-issue at best and as a value-added service at worst, the latter understands privacy features in terms of an application's functionality rather than its limitations. Under the latter approach, a data minimization requirement would therefore be viewed as a design challenge rather than a barrier to innovation. While it would be preferable for developers to embrace this approach willingly for the reasons set out above, the current commercial focus on the large-scale exploitation of personal information may make a legislative mandate along the lines of some of the new principles included in the proposed reform package for a new EU data protection regime[3] unavoidable.

Special attention should also be paid to the development of social norms regarding privacy in the online environment. In particular, greater emphasis should be placed on promoting an increased awareness of

[3] For example, the obligations on EU data controllers to ensure data protection by design and by default (Article 23, draft Data Protection Directive) and data portability (Article 18, Draft Data Protection Regulation).

information rights and obligations from early-years education for children (see, for example, Ewart and Tisdall 2012) to lifelong learning projects for so called "silver surfers". In considering our own moral framework at a very personal level, the question all of us should be encouraged to ask ourselves when processing our and others' personal information is not, "what do I want to do?", "what am I able to do?", or "what am I allowed to do?", but "what should (and shouldn't) I do?"

On a legal level, countries should consider adopting a consumer protection-style legal framework that moves away from the *caveat emptor* approach to the trade in personal information referred to above. Without restricting the individual's personal autonomy and their general right to share their personal information with others, the limitations of the current transparency approach should be acknowledged by placing legislative constraints on the processing activities to which individuals may lawfully consent and on the "other" legal grounds on which those processing activities may be justified. Mirroring established principles in consumer protection law, privacy statements that seek to authorize legally restricted processing activities should be capable of being declared void or voidable.

Finally and most importantly, public bodies should pay renewed attention to the overarching policy objectives that have always underpinned the fundamental right to privacy and data protection. Where those objectives override or are even necessary to support other objectives like administrative efficiency, national economic interests or national and public security, a self-denying ordinance should be imposed that prevents the unfettered access by public bodies to data held by other public bodies or by private entities or that at least limits such access to that which is absolutely necessary and proportionate. Measures to support such an approach would include much stronger constitutional restrictions on data use and data sharing, the strict imposition of a burden of proof on public bodies that access to and further processing of such data is necessary (rather than merely useful), as well as strict procedural requirements for obtaining such access in the form of warrants or court orders.

Given the current lobbying assault by large multi-national data controllers on the European Commission in the context of the review of the EU data protection regime, it is difficult to believe that the political will to carry out a root and branch examination of the need for a right to privacy is there. However, politicians and policy makers that now shy away from this difficult task may wish to review their position in light of the experiences made in recent years with regard to the global approach to a relaxing of the rules for the regulation of financial institutions. Short-terminism, while generally politically expedient, will almost always result in increased long-term risk and expense. The question is whether a loss of information privacy is a cost our societies can afford to bear.

References

boyd, danah and Alice E. Marwick. 2011. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. Paper presented at *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, September 2011. Available at SSRN: http://ssrn.com/abstract=1925128

Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (draft Data Protection Regulation), COM (2012) 11 final, Brussels, 25.1.2012

Department of Health and Social Security. 1984. Report of the Committee of Inquiry into human fertilization and embryology. Chaired by Dame Mary Warnock DBE. Available at http://www.hfea.gov.uk/docs/Warnock_Report_of_the_Committee_of_Inquiry_into_Human_Fertilisation_and_Embryology_1984.pdf

Edwards, Lilian and Ian Brown. 2009. Data Control and Social Networking: Irreconcilable Ideas? In: *Harboring data: information security, law and the corporation*, ed. Andrea Matwyshyn. Palo Alto: Stanford University Press.

Ewart, Carole and Kay Tisdall. 2012. *Embedding information rights in the primary and secondary education systems of the United Kingdom: Phase 2 report for the Information Commissioner's Office*, 31 March 2012. Available at http://www.ico.gov.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/embedding_information_rights_phase_2_report.ashx

German Constitutional Court. 1984. "*Census*" decision (in German), BverfGE 65, 1

Jenkins, Henry, Katie Clinton, Ravi Purushotma, Alice Robison and Margaret Weigel. 2006. *Confronting the Challenges of Participatory Culture: Media Education For the 21st Century*. Chicago: The MacArthur Foundation

Johnson, Bobbie. 2010. Privacy no longer a social norm, says Facebook founder. *The Guardian* online. Available at http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

Nissenbaum, Helen Fay. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Palo Alto: Stanford University Press.

Reding, Viviane. 2012. *The reform of the EU Data Protection Directive: the impact on businesses*. Speech delivered at the Business Summit Brussels, 18 May 2011. Available at http://europa.eu/rapid/press-release_SPEECH-11-349_en

Rooney, Ben. 2012. The Balance Between Open Data and Privacy. *Wall Street Journal*, online version, 12 September 2012. Available at http://online.wsj.com/article/SB10000872396390443884104577647600306243684.html

Simitis, Spiros. 1984. Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. *Neue Juristische Wochenschrift*, 394-405 (399).

Special Eurobarometer 359. 2011. *Attitudes on Data Protection and Electronic Identity in the European Union.* Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre. Available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Spiegel Online. 2012. *US Lobbyists Face Off with EU on Data Privacy Proposal*. Available at http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html

Vijayan, Jaikumar. 2012. Facebook email change sparks user outcry. *Computerworld* online. Available http://www.computerworld.com/s/article/9228538/Facebook_email_change_sparks_user_outcry