The normative shift: Three paradoxes of information privacy

Jockum Hildén

Abstract

While a tension between social norms of privacy, technology and law has always been present in debates on privacy law, the emergence of computerized databases in the 1970s shifted the focus of privacy law from publication to control over information flows. In the past decade, data flows have become increasingly globalized and personal communications digitized. This, in combination with advances in computing, allows for the creation of extensive databases that can be efficiently and automatically analyzed. The right to privacy is gradually being eroded by data processing activities that are often unknown to users of media, and communications technology which are rarely compatible with people's perception of privacy. The legislative attempts to overcome privacy challenges associated with these trends have regrettably resulted in paradoxical outcomes. First, a privacy paradox has evolved, which suggests that people's perception of their right to privacy is rarely an indication of awareness of the privacy consequences of their actions. Second, information privacy laws have introduced a transparency paradox, where the requirement of detailed privacy notices has resulted in less understanding of how personal data is used. Third, legislators in the EU have created a purpose paradox in their pursuit of facilitating the free movement of data while simultaneously aiming to protect the privacy of citizens.

Keywords: information privacy, data protection, European Union, socio-legal research, internet policy

---

Hildén, J. (2016) 'The normative shift: Three paradoxes of information privacy', pp. 63-73 in L. Kramp/N. Carpentier/A. Hepp/R. Kilborn/R. Kunelius/H. Nieminen/T. Olsson/P. Pruulmann-Vengerfeldt/I. Tomanić Trivundža/S. Tosoni (Eds.) *Politics, Civil Society and Participation: Media and Communications in a Transforming Environment*. Bremen: edition lumière.

1 Introduction

Privacy is a highly personal notion, which is hardly ever constant and always contested by new technologies and new settings, which means that generating a static legal definition of the right to privacy is difficult (see Nissenbaum, 2011; Cohen, 2012). Although this tension between social norms of privacy, technology and law has always been present in debates on privacy law, the emergence of computerized databases in the 1970s put significant emphasis on the role of information privacy.[1] Information privacy, or data protection, refers specifically to information on citizens rather than an abstract notion of what is considered private or intimate. Privacy guides what data are to be protected, but the information privacy frame focuses the discussion on the routine processing of personal data. In legal theory and policy research, information privacy relates to the access and control of information that is regarded as personal (Nissenbaum, 2010, p. 70). Access indicates when and how information about oneself is transmitted to a person or group, whereas control indicates who or what determines that access (see also Westin, 1967, p. 158). As people communicate personal information both voluntarily and involuntarily, access and control are rarely defined solely by the individual. When records were computerized they also became easier to transfer, which shifted the focus of privacy law from publication to control over information flows. Schwartz (2013, p. 1971) argues that the international debate on information privacy has always been about both human rights and data trade. Data trade does not, however, advance the privacy of a person, which generates an inherent tension in information privacy law. This tension has only become more apparent in the past decade, when data flows have been increasingly globalized and personal communications digitized, which allows for the creation of more extensive databases that can also be analyzed more efficiently due to advances in computing.

2 The normative shift

Privacy awareness, beliefs and actions to protect privacy vary a great deal between individuals, which means that any descriptive models of privacy must be extremely flexible (Burkart/Andersson Schwarz, 2013). Nevertheless, there are some common aspects of privacy that can be agreed upon within communities that form the basis of privacy law. Some social norms must thus be imagined to represent the "views of the nation" to such an extent that they

1 When I discuss European law specifically I will use the term "data protection," rather than "information privacy".

may be codified as law.[2] Although it would be unrealistic to state that privacy is a universal social norm that is more or less similar in all corners of the world, it can be argued that current privacy legislation originates from one single source, the US Bill of Rights from 1791. Although the ten Amendments to the Constitution do not explicitly mention privacy, the Fourth Amendment expresses the "right of the people to be secure in their persons, houses, papers, and effects" (USA, 1787).

A century later, privacy was explicitly defined by Warren and Brandeis (1890) as a right which "protect[s] the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds (p. 206)." The early privacy laws were torts that introduced compensation if the media had violated a person's privacy. The history of privacy legislation is thus concomitant with the development of media and communication technologies. Newspapers, pocket cameras, covert listening devices, video cameras and social networking sites have changed how people relate to the private sphere, blurred the public/private distinction, and at times created an urgent need for more legislation (Tene/Polonetsky, 2013). New technologies come into conflict with social norms of privacy and therefore instigate a need for more regulation, and vice versa: Uses of technology shape social norms, which may change how information privacy laws are interpreted by both courts and laymen.

Most privacy laws in the world are based on article 12 of the UN Declaration of Human Rights from 1948. Still, privacy law in general allows for quite wide-reaching exceptions. Laws, which aim to codify social norms of imagined communities (see Koskenniemi, 1990, p. 7), tend to be vague in order to avoid over-regulation and contain exceptions so that the laws themselves allow for divergence from rules without breaking the law (Koskenniemi, 2004). The inherent vagueness of human rights law creates an apparent challenge for information privacy legislation. Civic freedoms and rights have always been partially relinquished in exchange for security and access to valuable infrastructure in the modern bureaucratic state (Giddens, 1985). There must, however, be a balance between the interests of the public, such as security, and private interests, such as privacy. This was what impelled legislators to draft the first data protection laws in Europe in the 1970s. Activists and legal professionals were concerned that state-run computerized databases could be abused and required that safeguards be instated. The first countries to introduce data protection legislation were Germany, France, the UK, Sweden, Austria, Denmark, and Norway (Schwartz, 2013; Newman, 2008).

2 See Anderson's (2006) concept of nations as imagined communities.

As data flows are increasingly globalized, information privacy laws cannot be limited to the borders of nation states. The trade of personal information within Europe prompted the introduction of the EU Data Protection Directive in 1995. Countries with stringent data protection laws were concerned that multinational corporations were relocating their data processing activities to Belgium and Luxembourg, which lacked data protection laws altogether. Data protection authorities in the other European Community member states pushed for the inclusion of fairly strict data protection laws in order to protect the privacy of their citizens (Newman, 2008). However, since social norms of privacy are highly contextual and differ between communities and settings (Nissenbaum, 2010, p. 140), transnational information privacy legislation is challenging. Citizens from the different EU member states value aspects of privacy quite contrarily; whereas most EU citizens regarded financial information as personal data, the majority of Polish and Romanian citizens disagreed (EC 2011, p. 13). This particular challenge has been circumvented by not limiting the definition of personal data to certain categories of data, but whether or not that data can be linked to a person. This may however lead to a situation where data is retrofitted as personal data, "like an ideal gas to fit the shape of its container" (Ohm, 2010, p. 1741).

The legislative process of the Data Protection Directive shows how the focus of legislators in Europe has shifted from public to private processing of data. This shift has been advanced by the affordability of processing power and availability of data (Ohm, 2010). Powerful computers are available even to the smallest companies. In the retail industry, customer loyalty programmes are no longer merely about providing incentives and rewards to loyal consumers. As purchases are logged (in order to create databases of economic transactions), this data is used for targeted marketing and resold to so-called data brokers. The US data brokerage industry holds data points of over a billion transactions (FTC 2014).

The nature of data processing has shifted in volume, velocity, and variety, three key concepts which have been used to define big data (Laney, 2001). It is not only the sheer amount of data that has changed, but also the type of data. The right to privacy is therefore challenged by the fact that information which covers objective data, such as income or geolocation can be matched with more subjective data such as political views or even sexual preferences. Subjective data points have become more easily available since the digitization of personal communications. Social networking sites, personalized search engines, voice-over IP (VoIP), and instant messaging services facilitate the rendering of these latter data types. Users upload pictures of themselves online and share private information publicly, leading commentators to state that we live in a "post-privacy" world (e.g., Heller, 2008; 2010; 2011; Schramm, 2012). Still, that would be to gloss over questions of how infrastructure shapes

behaviour. The early online networks cherished anonymity; today's social networks reward identifiability. This evolution has created a wide gap between what data protection law recognizes as sensitive information, and what information social networking sites expect people to provide. For example, information on a person's political opinions, religious beliefs or sexual orientation are regarded as sensitive personal data, yet on Facebook they are categorized as "basic information" (Facebook, 2014); information which is very sensitive in many parts of the world.

Whereas uses of new technology challenge social norms of privacy, it is not these changes in behaviour that have influenced information privacy the most. Business practices which are unrelated to social norms, such as data mining and behavioural advertising, are driving regulatory change. The right to privacy is not only challenged by the nature of data that an organisation possesses, but also by what can be inferred from that data with statistical analysis (Ohm, 2010). These technologies are invisible to consumers and even go against social norms of privacy in ways that can be labelled as "creepy", although they are not illegal as such (Tene/Polonetsky, 2013, p. 2).

3 The paradoxes of information privacy

Few empirical findings would support the claim that privacy is an outmoded social norm. Instead, one can witness a "disconnect" between people's views on privacy and their actions (Andrejevic, 2015, Turow et al., 2015). Numerous studies in both Europe and the US show that people are increasingly worried about their online privacy, yet refrain from taking action which would secure their privacy in practice (Pew, EC 2015; Tan, 2011; Cobb, 2013; Turow, 2003; Debatin et al., 2009; Halbert/Larsson, 2015; Kennedy et al., 2015). This has been called the *privacy paradox* (Utz/Kramer, 2009).

According to Koskenniemi (2006), the international legal argument is often apologetic, construing the powers that be as fact and disregarding the word of the law, or utopian, construing the law as fact and disregarding actual power relations. The challenge lies in taking power relations into account without losing sight of the normativity of law. The post-privacy argument is inherently apologist, in that it merely accepts that privacy abuses are abundant and that the collection of data is highly unrestrained. Privacy activists, on the other hand, would often want to see all communications encrypted and all data processing subjected to the consent of individuals—something Obar (2015, p. 5) calls the "fallacy of data privacy self-management." The data management approach is further undermined by research that shows that even when

people are presented with a choice, the default settings should be seen as "de facto regulation" as they guide user behaviour to a large extent (Shah/Sandvig, 2008; see also Lessig, 2006).

Another paradox, which I call the *purpose paradox*, is the twin goal of information privacy legislation, as expressed here in the draft General Data Protection Regulation:

> 2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.
> 3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. (EC 2012: art 1(2; 3))

From the first article of the proposed Regulation one can thus deduce two goals: first, the free movement of data (within the EU) and second, the protection of information privacy. However, privacy scholars would argue that it is precisely the free movement of data which erodes the right to privacy (Ohm, 2010). How can this apparent paradox be explained? Surely the incompatibility of the two goals cannot be based on mere incompetence from the legislators, as data protection officials have been frequently consulted during the legislative process of the Regulation.

Privacy as such does not make room for business interests, as the International Covenant on Civil and Political Rights (UN, 1966: art. 4(1)) clearly states that derogations are necessary only "[i]n time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed". However, the European Convention of Human Rights (ECHR), ratified by all EU member states, does contain a reference to the national economy of a state:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Council of Europe, 1950: art. 8(2)).

The exceptions outlined in the ECHR outline some of the collective interests which can be invoked as reasons to limit the right to privacy. The processing of medical data is, for example, a prerequisite for the success of clinical trials. Privacy scholars are usually reluctant to discuss cases where denying privacy for social interests is not only reasonable but also preferable (Cohen, 2012, pp. 109, 116). It is still important to stress that the focus lies in the interest of the nation, which could also be equated with the public interest. In any case, the private interest(s) of corporations is undoubtedly secondary, if not outright incompatible with the right to privacy. It can also be argued that the interests of

a powerful corporation may in some cases be interpreted as the public interest. Nevertheless, the costs and benefits of the collection, processing and trade of personal information come at potential benefits for businesses and costs to individuals, which would argue for an interpretation of privacy which prioritizes the individual (Nissenbaum, 2010, p. 111). In information privacy law, this balance is no longer as clearly tilted in favour of citizens.

What is at hand is essentially a balancing act of apology and utopia – when legislators set to create the first data protection rules, data was already being processed and analyzed with the help of computers. When the debate evolved to include international transfers of data in the drafting stages of the EU Data Protection Directive, international transfers were already commonplace. Instead of simply accepting the situation, legislators created a legal document which recognized both transfers of data and the legitimate privacy claims of citizens. The purpose paradox was consequently introduced not because of the EU citizens' complex, contextual and relational approach to privacy, but the existence of unregulated business practice.

For this reason, information privacy law can be interpreted either by looking at the commercial advantages of data transfers or the value of limiting access to private information. Information privacy is fundamentally different from the negative right to privacy that requires the state to refrain from being intrusive, unless a crisis requires the state to limit that right. Information privacy is a positive right, which happens to recognize practices that both protect the rights of individuals and limits those rights at the same time. Freedom of expression has also been pointed out as a right which is in conflict with the right to privacy, and the legal system is partly grounded on conflicts of rights. The abnormal trait of information privacy is that this conflict is built into the right itself.

On the one hand, European information privacy entails principles on data minimization, consent and transparency (e.g. EC, 2012: art. 5; 7). Data minimization refers to *what* data may be retained and processed. The retention should not exceed the minimum level of data necessary in order to fulfil a function, be it cookies on websites or patient data in medical records. Consent is a requirement for when data may be processed. Even when data is easily obtainable, the data subjects should give their consent before processing. Exactly how consent is obtained is a question of great debate. It has been vividly discussed among practitioners and legal scholars, some of whom argue that consent can be given implicitly while other argue that there is no such thing as implicit consent, and that all consent should be explicit (e.g. EC, 2010). Transparency sets out principles for how the data should be processed. Data subjects should be made aware of how and for what purposes their data is used. The transparency requirement has been somewhat undermined, however, by the extensive use of highly complex End-User Licence Agreements (EULAs)

which outline how an entity is processing data. This has led to what Nissenbaum (2011, p. 36) calls a *transparency paradox*, according to which detailed privacy policies are less likely to be understood if they state all the possible conditions for the use of personal data.

On the other hand, there are principles which facilitate the free movement of data, such as the use of self-regulatory instruments and the encouragement of data protection authorities to cooperate (e.g. EC, 2012: ch. V). In theory, these concrete provisions are not each other's antithesis, and may coexist within the same legal documents. The provisions on self-regulatory instruments which facilitate international transfers do not threaten the protection of individuals on their own, however, their purpose is to advance the free movement of data which is a threat to the right to privacy in its own right. By introducing more and more systems that facilitate international transfers of data, the right to privacy is eroded.

4 Conclusion

While technological advances in the 20th century encouraged European legislators to introduce the concept of data protection, 21st century applications of 20th century innovations are proving to be even more challenging for the right to privacy. Notwithstanding government infractions as exemplified by the NSA and GCHQ scandals, private processing of personal data increasingly tests the right to privacy. The challenges are first and foremost introduced by technological innovations, but these innovations also affect our behaviour, and by extension, social norms.

The legislative attempts to overcome privacy challenges have unfortunately resulted in paradoxical outcomes. First, they have created a privacy paradox (Utz/Kramer, 2009), which suggests that people's perception of privacy is a poor indicator of awareness of the privacy consequences of their actions. Second, information privacy laws have introduced a transparency paradox (Nissenbaum, 2011), where privacy notices are counterproductive and bring about less understanding of data processing, not more. This implies that data controllers should go against the word of the law that requires detailed notice of data processing if the goal is that users would actually understand the notices. Third, and perhaps most importantly, legislators in the EU have created a purpose paradox in their pursuit of trying to enable the free movement of data at the same time as they aim to protect the privacy of the citizens of the EU.

These paradoxes are an expression of the apologist and utopian elements of information privacy: on the one hand, personal data is already being collected, processed and transferred across borders; on the other hand, personal data is an important element of the right to privacy and must be protected

despite these processing activities. However, it is worth noting that the challenges of information privacy are not a consequence of changing social norms, but evolving business practices that are largely unknown to users. Information privacy laws should for this reason become more grounded in the ideals of privacy rather than facilitate the reality of large-scale collection and transfers of data.

5 References

Andrejevic, M. (2015) 'Big data disconnects'. Paper for Data Power conference, University of Sheffield, June 2015.

Anderson, B. (2006) *Imagined communities: Reflections on the origin and spread of nationalism*, Revised Edition. London: Verso.

Bug, M. (2013) 'Societal divisions regarding attitudes towards digitized security measures? British versus German perspectives', pp. 159-174 in M. Löblich and S. Pfaff-Rüdinger (Eds.) *Communication and media policy in the era of the Internet*. Berlin: Nomos publishers.

Burkart, P., Andersson Schwarz, J. (2013) 'Post-privacy and ideology: a question of doxa and praxis', pp. 218-237 in A. Jansson and M. Christiansen (Eds.) *Media, surveillance and identity: A social perspective.* New York et al.: Peter Lang.

Cobb, S. (2013) 'Do consumers pass the buck on online safety? New survey reveals mixed messages', *We live security, 13.11.2013.* Downloaded on 14 May 2015 from http://www.welivesecurity.com/ 2013/11/13/do-consumers-pass-the-buck-on-online-safety-new-survey-reveals-mixed-messages/.

Cohen, J. E. (2012) *Configuring the networked self: Law, code, and the play of everyday practice.* Cumberland, RI, USA: Yale University Press.

Council of Europe (1950) 'European convention for the protection of human rights and fundamental freedoms, as amended by protocols nos. 11 and 14', 4 November 1950, ETS 5. Downloaded on 10 September 2015 from http://www.refworld.org/docid/3ae6b3b04.html.

European Commission (2011) 'Flash Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union'. Downloaded on 12 November 2014 from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

European Commission (2010) 'Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union (Brussels: 4.11.2010)', COM(2010) 609 final.

Federal Trade Commission (2014) 'Data brokers: a call for transparency and accountability'. Downloaded on 1 January 2015 from https://www.ftc.gov/system/files/documents/reports/ data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Giddens, A. (1985) *The nation-state and violence: Volume two of a contemporary critique of historical materialism.* Cambridge: Polity Press.

Heller, C. (2008) 'Embracing post-privacy'. Presentation at 25th Chaos Communication Congress. Berlin, Germany. December 29. Downloaded on 10 June 2015 from http://events.ccc.de/congress/2008/Fahrplan/attachments/1222_postprivacy.pdf.

Heller, C. (2010) 'Die Ideologie Datenschutz'. Carta [March 17]. Downloaded on 17 July 2015 from http://carta.info/24397/die-ideologie-datenschutz/.

Heller, C. (2011) *Post-Privacy: Prima leben ohne Privatsphäre*. Munich: Verlag C. H. Beck.

Kennedy, H., Elgesem, D., Miguel, C. (2015) 'On fairness: User perspectives on social media data mining', *Convergence:* 1-19, doi:10.1177/1354856515592507.

Koskenniemi, M. (2006) *From apology to utopia: The structure of international legal argument.* Reissue with a New Epilogue. Cambridge: Cambridge University Press.

Koskenniemi, M. (2004) 'International law and hegemony: A reconfiguration', *Cambridge Review of International Affairs*, 17(2): 197-218.

Koskenniemi, M. (1990) 'The politics of international law', *European Journal of International Law,* 1(1). Downloaded on 25 August 2015 from http://ejil.org/pdfs/1/1/1144.pdf.

Laney, D. (2001) '3D data management: Controlling data volume, velocity and variety', *Meta Group/Gartner.* Downloaded on 14 November 2014 from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lessig, L. (2006) *Code: version 2.0.* New York (N.Y.): Basic Books.

Michalis, M. (2007) *Governing European communications*. Lanham, MD: Lexington.

Newman, A. L. (2008) 'Building transnational civil liberties: Transgovernmental entrepreneurs and the European data privacy directive', *International Organization,* 62(1): 103-130.

Nissenbaum, H. (2011) 'A contextual approach to privacy online', *Daedalus,* 140: 32-48. Downloaded on 10 May 2015 from http://www.amacad.org/publications/daedalus/ 11_fall_nissenbaum.pdf.

Nissenbaum, H. (2010) *Privacy in context.* Stanford: Stanford University Press.

Obar, J. A. (2015) 'Big data and the phantom public: Walter Lippmann and the fallacy of data privacy self-management' [August 20, 2015]. Downloaded on 1 September 2015 from http://ssrn.com/ abstract=2239188.

Ohm, P. (2010): 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review,* 57(6): 1701-1777.

Schramm, J. (2012) *Klick Mich: Bekenntnisse einer Internet-Exhibitionistin*. Munich: Knaus.

Schwartz, P. M. (2013) 'The EU-U.S. privacy collision: A turn to institutions and procedures', *Harv. L. Rev.,* 126(7): 1966-2013.

Shah, R. C., Sandvig, C. (2008) 'Software defaults as de facto regulation: The case of the wireless Internet', *Information, Communication & Society,* 11(1): 25-46.

Tan, M. (2011) 'Can online privacy policy help to prevent the intrusiveness in data collection?'. Paper for IAMCR 2011.

Tene, O., Polonetsky, J. (2013) 'A theory of creepy: Technology, privacy and shifting social norms', *Yale Journal of Law & Technology.* Downloaded on 10 November 2014 from http://ssrn.com/abstract=2326830.

Turow, J., Hennessy, M., Draper, N. (2015) 'The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation'. Downloaded on 30 June 2015 from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

UN General Assembly (1966) 'International covenant on civil and political rights' [16 December 1966], United Nations, Treaty Series, 999: 171. Downloaded on 10 September 2015 from http://www.refworld.org/docid/3ae6b3aa0.html.

United States of America (1787) 'Constitution [United States of America]', [17 September 1787], Downloaded on 28 September 2015 from http://www.refworld.org/docid/3ae6b54d1c.html.

Utz, S., Kramer, N. (2009) 'The privacy paradox on social network sites revisited: The role of individual characteristics and group norms', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 3(2), article 1. Downloaded on 10 August 2015 from http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1.

Warren, S. D., Brandeis, L. D. (1890) 'The right to privacy', *Harv. L. Rev*, 4(5): 193-220.

Westin, A. F. (1967) *Privacy and freedom*. London: Bodley Head.

Biography

Jockum Hildén is a PhD Candidate in Media and Global Communications at the Department of Social Research, University of Helsinki, Finland. In his dissertation he studies the evolution of data protection policy in the EU by examining the legislative process of the new General Data Protection Regulation. The research aims to assess the influence of interest groups on information privacy policy and ascertain whether or not their efforts have affected the regulatory output of the EU institutions.

Contact: jockum.hilden@helsinki.fi