Final version published: http://download.springer.com/static/pdf/137/art%253A10.1007%252Fs10676-016-9395-z.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs10676-016-9395-z&token2=exp=1462277734~acl=%2Fstatic%2Fpdf%2F137%2Fart%25253A10.1007%25252Fs10676-016-9395-z.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Farticle%252F10.1007%252Fs10676-016-9395-z*~hmac=6e9dc807760356951c20d6cf2a3054e3771139b63d1646bc09ea6290e8eae8fa

B. van der Sloot[1]

Introduction

Origins of the special issue

Privacy is the topic of this special issue of *Ethics and Information Technology*. It contains seven original articles that were presented at the Amsterdam Privacy Conference 2015 (APC2015), which was held from 23-26 October 2015 in Amsterdam. APC2015 is a biennial conference organized by the Amsterdam Platform for Privacy Research (APPR), a group consisting of more than 70 researchers at the University of Amsterdam who are involved with privacy aspects in their daily activities. They approach the topic from different angles, such as law, philosophy, economics, computer science, medicine, communication studies and political science. Through an interdisciplinary approach and joint discussion, APPR increases both the understanding and awareness of privacy issues. APPR organizes workshops, symposia, conferences and educational programs such as the minor Privacy Studies.

APC2015 hosted over 200 (paper) presentations and included keynote lectures by, inter alia, Helen Nissenbaum, Max Schrems, Viktor Mayer-Schonberger, Amitai Etzioni, Julie Brill, Anita Allen, Latanya Sweeney, Gabriella Coleman, Ronald Plasterk, Ashkan Soltani and Deirdre Mulligan. The parallel sessions where roughly divided in seven tracks: the Commercial Value of Privacy, Privacy and Healthcare, Privacy in the Information Society, Privacy and Security, Privacy and Technology, the Value and Ethics of Privacy and the Transformation of the Public Space and Personalized Communication. The seven papers for this special issue where mostly taken from the Value and Ethics of Privacy track.

Three characteristics distinguished APC2015 from other privacy conferences. First, the conference was fully interdisciplinary. Second, the conference aimed at societal relevance by building bridges between academics, regulators, civil society and companies and between different countries and continents. Real and concrete privacy problems were at the heart of the keynote sessions – the parallel sessions revolved around signalling these and future problems and aimed to provide solutions and viable alternatives. Finally, APC2015 provided plenary sessions aimed at an international and interdisciplinary public, and small scale and interactive parallel sessions, with an average number of 20 to 30 participants, which allowed for in-depth discussions among peers.

Privacy: a broad and elusive concept

[1] Bart van der Sloot is a researcher at the Institute for Information Law (IViR) at the University of Amsterdam, the Netherlands, and the coordinator of the Amsterdam Platform for Privacy Research (APPR).

The interdisciplinary nature of privacy research is partly necessitated by the broadness and elusiveness of the topic. It has been said that privacy is the only right on which there is not even agreement on the pronunciation (referring to the difference in British and American tongue). Indeed, there is no standard definition of 'privacy' as of yet. Some scholars focus on control over personal data, others on access to private spaces, some on bodily integrity, others on communicational secrecy, some on relational privacy, others on seclusion, etc. In fact, privacy seems to function as an umbrella term for several quasi-related matters. There is also no consensus in literature on what the value of privacy is. Some argue that it has an intrinsic value,[2] others that it is instrumental in relation to other values and still others have claimed that privacy is in fact a redundant concept.[3] Even scholars that agree on the fact that privacy should be seen as having an instrumental value disagree on which value it is instrumental to, either pointing to negative freedom,[4] positive freedom,[5] human dignity,[6] individual autonomy[7] or the development of one's personality.[8]

There is also a big cultural difference with respect to the value and meaning of privacy. Historically, the meaning of privacy has changed quite substantially. Every epoch seems to have a different approach to privacy and what is regarded as private, not in the last place, because the boundaries between the public and private domain constantly shift.[9] Around the globe, privacy is perceived quite differently, depended as it is on local and cultural traditions. For more communal societies, such as native tribes[10] and, to a certain extent, communist regimes,[11] the private domain and individual privacy have a quite different meaning than for most western societies.[12] Still, even in the western world, there are contrasting approaches among the various jurisdictions. The most prominent right now is the divide between Europe and the United States of America. While in Europe, data protection is seen as a fundamental right, in the USA, processing personal data is primarily regarded in economic terms.[13]

The European Union has embedded quite strict rules on the processing of personal data in the Data Protection Directive.[14] That directive holds that data may in principle not be

---

[2] See for an explanation: D. J. Solove, 'Understanding privacy', Cambridge, Harvard University Press 2008.
[3] J. J. Thomson, 'The Right to Privacy', Philosophy & Public Affairs 4, no. 4, I975.
[4] W. von Humboldt, 'The limits of state action', London, Cambridge University Press, 1969. J. S. Mill, 'On liberty', Norton, New York, 1975.
[5] Roe v. Wade, 410 U.S. 113, 1973.
[6] S. I. Benn, 'Privacy, Freedom, and Respect for Persons', p. 223-244. In: F. Schoeman (ed.), 'Philosophical Dimensions of Privacy: an Anthology', Cambridge University Press, Cambridge, 1984.
[7] B. Roessler, 'The value of privacy', Polity Press, Cambridge, 2005.
[8] This seems the approach taken by the European Court of Human Rights: B. van der Sloot, 'Privacy as personality right: why the ECtHR's focus on ulterior interests might prove indispensable in the age of Big Data', Utrecht Journal of International and European Law, 2015.
[9] P. Ariès & G. Duby, 'A history of private life', Cambridge, The Belknap Press of Harvard University Press, 1987-.
[10] S. Van der Geest, 'Toilets, privacy and perceptions of dirt in Kwahu-Tafo'. In: S.van der Geest and N.Obirih-Opareh (eds), 'Toilets and Sanitation in Ghana: An urgent matter'. Accra: Institute of Scientific and Technological Information(INSTI), CSIR , 2001. S. Van der Geest, 'Thetoilet: Dignity, privacy and care of elderly people in Kwahu, Ghana'. In: S. Makoni & K. Stroeken (eds), 'Ageing in Africa: Sociolinguistic and anthropological approaches', Aldershot: Ashgate, 2002.
[11] See among others: S. L. Levitsky, 'Copyright, Defamation, and Privacy in Soviet Civil Law', Sijthoff & Noordhoff, Alphen aan de Rijn, 1979.
[12] Although communitarians would hold differently: A. Etzioni, 'The limits of privacy', New York, Basic Books, 1999.
[13] Charter of fundamental rights of the European Union (2000/C 364/01). <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.
[14] 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 and on the free movement of such data.

transferred to other countries if those countries cannot guarantee an adequate level of protection.[15] The European Commission had adopted a safe harbour agreement, in which it declared that the USA did actually provide an adequate level of protection.[16] Max Schrems, an Austrian citizen, however, challenged that decision and submitted a complaint. After a lengthy juridical procedure, the European Court of Justice declared the decision by the European Commission invalid.[17] There are now transatlantic negotiations going on in order to develop new rules in order to legitimize the transitional data flows. If these negotiations fail, most data-traffic by companies, government organisations and also citizens between Europe and the United States cannot be deemed legitimate unequivocally.

The interdisciplinary nature of privacy

Consequently, the meaning and interpretation of privacy depends on the epoch, the culture and the philosophical approach to it. Moreover, personal differences play an important role. Something that one person may perceive to be very private (for example, one's income or nude pictures), could be things that others easily disclose. This variety is also reflected in the many different (academic) fields for which privacy has a certain relevance. While philosophers aim to define the value of privacy, legal scholars approach privacy as a right and fundamental claim of the individual against the state, a business and even other individuals. In anthropology, researchers investigate the various meanings of privacy in different cultures, while in medicine, doctor-patient confidentiality and the protection of sensitive information are central themes.

In informatics and computer science, designing the technical infrastructure of information systems to implement privacy by design and privacy enhancing technologies is one of the prominent fields of research, as is, of course, the protection of personal data against hacks and data leaks. Media and communication science investigates, inter alia, whether and if so how citizens are influenced in their behaviour by personalized communication, a theme that is also increasingly prominent in political science, ever since the Obama-campaign has introduced similar techniques to influence voter-behaviour. In archival science, the discussion revolves around keeping as many relevant sources of information about citizens and institutions, while at the same time trying to abide by the rules on privacy and data protection. In surveillance studies, a prominent issue is the relationship between mass surveillance by intelligence services and the respect for fundamental human rights. These are but a few of the disciplines involved with privacy research.

Increasingly, scholars are also engaging in interdisciplinary research, as it is believed that only through interdisciplinary research, current privacy problems can be fully understood and tackled. Now, perhaps more than ever, privacy is under pressure due to numerous technological developments. For example, the private and the public domain seem to converge. On the one hand, the private lives of people are increasingly taking place in the public domain. Reference can be made, inter alia, to the smart phones many people permanently carry with them.[18] On the other hand, the private realm is increasingly chipped and wired in order to run smart devices and intelligent applications. To provide a further

[15] Article 25 Data Protection Directive.
[16] 2000/520/EC Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) Official Journal L 215 , 25/08/2000 P. 0007 – 0047.
[17] European Court of Justice, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, In Case C-362/14, 6 October 2015.
[18] See also: Supreme Court of the United States, Riley v. California, No. 13–132. Argued April 29, 2014—Decided June 25, 2014.

example, the physical body seems no longer the only body people have. Indeed, for a new generation, virtual bodies and online personas and reputations are just as important as the integrity of one's physical body. These are but a few of the technological developments that challenge old and established ideas about privacy.

Developments such as the Electronic Patient Files, the Quantified Self Movement and Big Data analytics all have technical, juridical and ethical aspects to the them and often have relevance for other disciplines as well, such as medicine, sociology and political science. Consequently, to fully understand such topical developments and find new and innovative solutions, scholars often find themselves challenged to engage in multidisciplinary research, looking beyond their own field or discipline and working together with colleagues form other branches and faculties. This also holds true for the articles in this special issue. Most of the authors of the seven articles contained in this special issue address topical societal issues that affect or involve privacy and try to find new and innovative solutions through a multidisciplinary approach.

Content of this special issue

In her article *'The Transparent Self'*, Marjolein Lanzing discusses the ethics of self-tracking and the notion of the Quantified Self. In particular, her paper focuses on a conceptual tension between the idea that disclosing personal information increases one's autonomy and the idea that informational privacy is a condition for autonomous personhood. She argues that while self-tracking may sometimes prove to be an adequate method to shed light on particular aspects of oneself and can be used to strengthen one's autonomy, self-tracking technologies often cancel out these benefits by exposing too much about oneself to an unspecified audience, thus undermining the informational privacy boundaries necessary for living an autonomous life. As the practice of self-tracking becomes increasingly institutionalized, users will increasingly be able to "outsource" their self-government to devices and those who control and access them by making visible what was not visible before.

Lanzing's thesis is that extended transparency conflicts with the informational privacy norms necessary for full autonomy. Success stories about empowerment, self-control and self-improvement camouflage the reality of decontextualization. The broader privacy problem of decontextualization deserves further normative scrutiny, yet, it must also be discussed how to practically negotiate the tension between transparency and limits on disclosure. Users should be educated about digitalization of cultural practices, information flows of emerging self-tracking technologies, potential purposes of one's information and potential audiences, Lanzing argues. Furthermore, the design features of self-tracking technologies could be critically evaluated and alternatives could be offered, beyond the mere option of 'consent', whereby users have granular control over the flow of their information and the potential audiences able to access their data. Users should also be able to anonymize or delete their data, Lanzing suggests.

In her article '*Remembering Me: Big Data, Individual Identity, and the Psychological Necessity of Forgetting*', Jacquelyn Burkell discusses the working of the internet in terms of remembering and what impact the internet has on the development of one's identity. Every individual has a personal narrative, she argues, a story that defines someone. A strong sense of identity is rooted in a personal narrative that has coherence and correspondence: coherence in the sense that the story is consistent with and supportive of one's current version of 'self'; and correspondence in the sense that the story reflects the contents of autobiographical memory and the meaning of experiences. These goals are achieved by a reciprocal interaction of autobiographical memory and the self, in which memories consistent with the self-image are reinforced, in turn strengthening the self-image they reflect. Thus, personal narratives

depend crucially on the malleable nature of autobiographical memory: a strong sense of self requires that one remember what matters, and forget what does not.

Today, Burkell suggests, anyone who is active online generates a highly detailed, ever-expanding, and permanent digital biographical 'memory'– memory that identifies where a person goes, what that person says, sees and does in increasing detail as physical lives become more and more enmeshed with electronic devices capable of recording communications, online activities, movements, and even bodily functions. Burkell's paper explores the consequences of this digital record for identity, arguing that it presents a challenge to a person's ability to construct personal narratives – narratives that are central to a sense of 'self'. She concludes by suggesting that forgetting should be reintroduced into the biographical archive in order to redress the technologically-induced shift, having the effect that for the first time in history, 'save' has become the default. An 'expiry date' might be required; if the expiry date passes without further action, the information is rendered inaccessible. Another option, Burkell suggests, could be to rely on a range of algorithmic strategies such as erasing, blurring, aggregating, injecting noise, data perturbing, masking, and so on that would be used to 'upset' the life-log records. Their goal is to build in 'necessary processes' of forgetting modeled on the natural forgetting that characterizes biological memory.

In his article '*Big Data: Finders Keepers, Losers Weepers?*', Marijn Sax discusses the legitimacy of Big Data processes. With the arrival of Big Data, data are often lauded as 'the new oil' or as 'goldmine' from which 'nuggets of gold' can be retrieved. Advanced data mining techniques allow companies to generate non-trivial new insights out of existing data. Since collecting more data always translates itself into more potential new insights waiting to be extracted from the data, data hungriness is a structural condition of the big data world, according to Sax. Looking at the conduct of typical Big Data companies, Sax argues that their success is largely dependent on their ability to generate new, non-trivial insights out of existing data. Besides this ability to create new insights (and one may even say new data) out of existing data, the business model of companies is also premised on the fact that creators of these new insights may *appropriate* these new insights.

Sax discusses in detail whether this *ethical* judgment is a legitimate one. Straightforward as it may sound, he believes that the legitimacy of this act of appropriating newly created insights essentially depends on the implicit acceptance of a 'finders, keepers' ethic. Once this implicit acceptance of a 'finders, keepers' ethic is made explicit, it turns out that this 'finders, keepers' ethic itself depends on various implausible assumptions. As a result, it is far from obvious that the business of Big Data companies is legitimate from an ethical point of view. Against the background of potential threats of Big Data, this analysis could function as an additional basis of critique, highlighting the problematic normative presuppositions of Big Data companies' entrepreneurial conduct. Ultimately, this may have legal and political consequences concerning the regulation of big data companies.

Titus Stahl, in his article, '*What's wrong with indiscriminate mass surveillance? From individual liberty to political power*', discusses the value of privacy and the approach to privacy violations in Big Data or mass surveillance type of data processing activities. Stahl argues that recent disclosures suggest that many liberal democratic governments apply indiscriminate mass surveillance technologies that allow them to capture and store massive amounts of communications of citizens and of non-citizens alike. His article argues that traditional liberal critiques of government surveillance that center on the individual right to privacy only incompletely capture the harm that is caused by the application of such technologies as they ignore their distinctive political dimension. As a complement to standard liberal approaches to privacy, the article develops a critique of surveillance that focuses on the question of political power.

On the proposed account, surveillance is an exercise of political power that must be checked to allow the existence of an autonomous public sphere that imposes constraints even in cases where no individual rights are violated. Stahl suggests that indiscriminate mass surveillance not only often threatens individual liberty and non-domination and undermines valuable non-political relationships, but that it also intrinsically constitutes a form of exercise of political power over the public sphere that is incompatible with the idea of democratic self-determination. In contrast to the liberal theories, an account that builds on a conception of public power can show why not only information use but already information capture and storage are problematic. This is because such practices amount to a change of the environment of social relationships and thereby of those relationships and the roles that are created by them – independently of whether those subject to it know about it. Furthermore, it acknowledges not only individual but also collective interests and it accounts for the intuition that surveillance of political communications causes a particular kind of harm. Consequently, Stahl concludes, the government use of surveillance technologies in the public sphere must be appropriately restricted so that surveillance-free spaces of public deliberation remain available which allow both for small-scale (e.g. for activist groups) and large-scale group deliberation.

Adam Moore, in '*Privacy, Speech, and Values: What we have No Business Knowing*', tackles the difficult subject of reconciling the right to privacy and the freedom of speech. He suggests that in the United States, the ascendancy of speech protection is due to an expansive and unjustified view of the value or primacy of free expression and access to information. This is perhaps understandable, given that privacy has been understood as a mere interest, whereas speech rights have been seen as more fundamental. Moore, however, feels that the "mere interest" view of privacy is false. Privacy, properly defined, is a necessary condition for human well-being or flourishing. In his contribution, he sketches several of the dominant argument strands that have been offered in support of presumptively weighty speech rights. While these arguments, taken together, establish that free speech is important, they do not support the view that speech should nearly always trump privacy.

Moore suggests that at one extreme, political, philosophical and social arguments suggest that information is clearly important for self-government while at the other, communication is said to reflect little or no social value. This range corresponds to high-value, low-value, and no-value speech. Nevertheless, just because some expression has been deemed high-value with clear public importance does not mean that privacy, or other speech restrictions like property or contracts, are automatically set aside. Moore suggests that the freedom of expression, suitably defined, and privacy should be viewed as having equal weight. Moreover, in cases of conflict, privacy and speech should be balanced in a way that promotes both of these important values. In his article, Moore develops several standards to guide the balancing process in order to properly assign weights and balance those weights appropriately.

In '*Personal information as communicative acts*', Jens-Erik Mai extends previous accounts of informational privacy as contextual. Where previous accounts have focused on interpretations of the privacy context itself as being contextual and open for negotiation, his paper extends those analyses and shows that personal information itself is in fact best understood as contextual and situational - and as such open for interpretation. The paper reviews the notion of information as it has been applied in informational privacy and philosophy of information, and suggests that personal information ought to be regarded as communicative acts. The paper suggests a reconceptualization of informational privacy from focus on controlling, limiting, or restricting access to material carriers of information to a focus on a regulation of the use, analysis, and interpretation of personal information.

Mai argues that information can be understood in two fundamental different ways. One approach understands information as true representation of reality, and another approach understands information as signs of reality that is open for interpretation and negotiation. In the first approach, personal information is like *natural* meaning (spots that mean measles); data, traces, and footprints are viewed as true representations of state of affairs, and the challenge is to control the flow of the material that carries information. In the second approach, personal information is like *non-natural* meaning (rings on the bell that mean that the bus is full); data, traces, and footprints are viewed as signs open for interpretation and negotiation, which only make sense in specific contexts and situations through conventions. Privacy theories in the first tradition focus on controlling, limiting, or restricting access to the material carrier of information, while those in the second tradition focus on pragmatics of the information and of the situation; the aim is to regulate use, analysis, and interpretation of personal information.

Finally, Marc-André Weber, in his paper '*Privacy: An Institutional Fact'*, aims to determine what kind of facts are "the fact of being private" and "the fact of being public". Weber uses Searle's way of speaking and asks: are they brute facts, i.e. elements of physical reality, or institutional facts, i.e. elements of social reality? At first sight, it may seem obvious that one should answer the latter question affirmatively and the former question negatively, Weber suggests. But this answer is more problematic than it seems. Brute fact and institutional facts have the same "texture": they are facts. Therefore, it is easy to confuse them in discussion, because in both cases speech is descriptive. Moreover, this confusion is often found in debates about privacy, but it is rarely addressed.

Naturalistic views about privacy, which Weber calls a "brute fact account", are frequently found in such debates. Weber suggests that although it seems that if everyone knows about P, then the public knows, and therefore P is public, this intuition must be rejected because it relies on a confusion between a brute fact and an institutional fact. "Everyone" refers to a brute fact: a group of people. "The public" refers an institutional fact. So, "everyone knows about P" does not equate to "the public knows about P", because they refer to different layers of reality. People count as the public only when it is legally permissible for them to learn about something. If this is not the case, for example when they spread gossips, they do not count as the public, but only as a group of private individuals.

Moral conservatism and the way forward

Privacy scholars are often accused of moral conservatism and indeed, there seems a constant tension between new technologies and applications on the one hand and privacy protection on the other hand. New technologies such as Big Data analytics ensure that massive amounts of (personal) data may be gathered, analyzed and used. The internet stores millions of bytes and digits per second and archives them in a quasi-permanent way. Through the internet of things, every object may in time be censored, connected to the internet and designed in such a way that it can gather about every piece of information there is to know, whether it is movement, weight, sound, light or other factors that a device is set to measure. Combined with smart technologies, the immense data gathering processes may be used for smart television, smart cities and smart refrigerators and will in the future increasingly be applied in the healthcare sector for smart robotics, total genome analysis and more. The Quantified Self Movement, in a way, is the internet of people, the third generation of the internet. While at first, people went *on* the internet, the internet of things meant that objects could be connected *to* the internet. Now, increasingly, people are also connected *to* the internet (as though their bodies where objects). Mass surveillance

activities by states are facilitated by camera's on the corners of many city streets, by data retention activities storing most -if not all- internet traffic and by the possibility to gather meta-data and derive from them very detailed pictures of people's lives and the content of their communications.

Of course, such new developments can produce enormous benefits. Safety can be increased by surveillance activities, healthcare can be both cheaper and more effective, smart devices can make the lives of citizen's more convenient and less burdensome, self-tracking can lead to more knowledge and self-awareness, the internet of things can promote transparency, social networks can foster connectivity, cloud computing can ensure efficiency, etc. However, these technologies also have potential negative effects. People's informational privacy may be at stake, since individual autonomy and personal freedom may be undermined by technologies that enable steering and influencing people's behavior. States and businesses may abuse their power and even if they don't, the power-imbalance itself can ensure that citizens restrict their behavior (the chilling effect). People may be nudged - they may be persuaded to buy certain products, read certain online content and even, vote a certain political party through personalized communication. These are but a few of the many positive and negative effects that the new technologies bring with them.

Currently, the division of roles seems suspiciously clear. Large internet companies such as Google, Facebook and Apple, leading Big Data enterprises, intelligence agencies and governments around the globe promote the use of data gathering techniques for purposes of personalized advertising, group profiling, mass surveillance and the likes. They rely on these new technologies and often defy the lack of evidence that these techniques actually work. To provide just one example, it is as of yet unclear whether and if so, to what extent the mass surveillance activities by national intelligence services actually promote national security. Many have argued that they are simply not the right tool for finding terrorists and some agencies have in fact abandoned large scale data processes and have gone back to 'old-fashioned' spies and intelligence personal on the ground, as they believe that to be more effective. Moreover, the potentially negative effects on the privacy, freedom, autonomy and dignity of people are mostly ignored or set aside as the interests at the other side of the spectrum, whether national security, economic efficiency or freedom of speech, is said to be more important or, in any case, outweigh the right to privacy and data protection.

Privacy scholars feel pressured to provide counterweights to this trend, as is also evidenced by this special issue. Although self-tracking might provide more knowledge and self-awareness, it could also undermine personal autonomy, warns Lanzing. Big Data thrives on a 'finders, keepers' ethics, says Sax, but in fact this ethics is inapplicable to new data technologies and so, Big Data processes often lack legitimacy. Privacy is often outweighed by freedom of speech, but in fact, should be seen as just as weighty, argues Moore. For ages, identity and personal development have been (partially) dependent on the virtue of forgetting, while the internet might disrupt this fact. That is why, Burkell argues, the internet should be changed and adapted (in part) to how people have been living, prior to the existence of the Internet. Because liberal ethics is unable to explain why mass surveillance is problematic, one must turn to other (republican) theories to do so, argues Stahl. And even Weber's more descriptive paper is based on a distinction between 'private' and 'public', a distinction that seems to become more superfluous with the day.

Obviously, all of these are important points to make, especially given the one-sidedness of the arguments put forward by many businesses and states. And these points are made as eloquent and energetic as one could hope for. Still, it is also important that the discussion moves to a next stage for two reasons. First, it is important that privacy scholars do not become equivalent to well-read privacy advocates. It is seldom to never that one

hears a privacy scholar say that mass surveillance is actually a fantastic benefit for modern society, that Big Data processes are legitimate, that new technologies like self-tracking might actually improve a person's autonomy or that it is right that in many cases, national security or freedom of expression outweighs privacy. It is important that privacy academics remain neutral and objective. They should not only stress the importance and value of privacy and merely attack new technologies and social developments that might potentially undermine it. In time, it would be good if the antagonism between pro and con would be diminished.

Secondly, the value and meaning of privacy is constantly changing. As explained, the understanding of privacy is in many ways tied to societal and technological developments. The most interesting question right now seems whether and if so, how the concept and meaning privacy will (need to) change yet again. The traditional distinctions between the private and the public, between the self and the other and between the physical and the virtual reality are increasingly blurring. Furthermore, many of other concepts and distinctions that were considered unproblematic for decades are currently challenged. To give an example, many ethical and juridical assessments revolve around the idea of 'personal data', which signifies data with which someone can be identified.[19] This is contrasted not only with non-identifying information, but also with sensitive personal data (regarding, for example, health, political and sexual preferences and race), which most commentators agree upon deserve a higher level of protection. It is, however, questionable whether such concepts are still tenable in the Big Data era, not only because the individual element and the individual interests in these types of processes are often incidental and difficult to specify, but also because the categorization of types of data only work in a world where the status of data is relatively stable. However, in reality, the nature of the data is becoming less and less static and data go through a circular process: data are linked, aggregated and anonymized and then again de-anonymized, enriched with other data and profiles, so that they become personally identifying information again, potentially even sensitive data – subsequently, they may be pseudonymised, used for statistical analysis and group profiles, and so on. Consequently, instead of categorizing types of data and making distinctions between personal data, sensitive data, private data, statistical data, anonymous data, non-identifying information and meta data, it could be worthwhile to try and develop a new, more hybrid and circular approach to the value of data.

These kind of questions will hopefully get even more attention from privacy scholars in the future. If *Ethics and Information Technology* would consider publishing a special issue on privacy in two or three years from now, new questions that could be addressed are: does the concept of 'personal data' hold in the age of Big Data; is it still viable to focus on one or a selected group of parties as responsible (as bearing the moral or legal burden) for data processing activities, while in reality, data constantly flow between different parties, databases are increasingly merged and it is often unclear where the data being processed came from originally, how they were collected and by whom; is it still viable to maintain the distinction between the private and the public domain or could it prove potentially interesting to develop a more hybrid moral, legal and social understanding of the public and private sphere; similarly, is the distinction between the real and the digital world, the physical and virtual body, still viable 10 years from now, or could it prove potentially interesting to move towards a more hybrid moral, legal and social understanding of the real and the virtual; does it still make sense to develop one's identity based on the idea that the past will be (party) forgotten, or is it imaginable that in time, identities and personalities will be developed even

[19] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, 20 June 2007, Brussels.

though most information about peoples' lives are recorded, stored and analyzed on a quasi-permanent basis; is it still viable to regard autonomy as something individual, or is it possible to move towards a concept in which individual autonomy is intertwined with and partially depended on the aid and knowledge of not only others, but also of machines and robots?

These are but a few of the questions that lie ahead and will keep the great minds of the scholars writing for this special edition and the next generation busy. Doing so, the reaction of privacy scholars towards new societal and technological developments will hopefully not only be defensive, they will not only argue that current practices are illegal or unethical, undermine one's individual autonomy or personal freedom or should be changed in order to reflect how we have lived and understood ourselves for centuries. Rather, they will also challenge and rethink the very fundaments of how people have lived for ages, how the standard approach has been to individual autonomy, informational privacy, personal freedom, human dignity and human flourishing and whether it needs to be changed in order to adequately address the new challenges the technological developments trigger.