Elisa Orrù

Minimum Harm by Design

Reworking Privacy by Design to mitigate the risks of surveillance

Pre-print version

Final version published in:

R. Leenes et al. (eds.), Data Protection and Privacy: (In)visibilities and Infrastructures, Law, Governance and Technology Series 36, Springer 2017, 107-137

DOI 10.1007/978-3-319-50796-5_5

Abstract

Particular applications of Privacy by Design (PbD) have proven to be valuable tools to protect privacy in many technological applications. However, PbD is not as promising when applied to technologies used for surveillance. After specifying how surveillance and privacy are understood in this paper, I will highlight the shortcomings of PbD when applied to surveillance, using a web-scanning system for counter-terrorism purposes as an example. I then suggest reworking PbD into a different approach: the Minimum Harm by Design (MHbD) model. MHbD differs from PbD principally in that it acknowledges that the potential harms of surveillance bear not only upon privacy but also values that define the very constitution of a society and its political character. MHbD aims to identify and systematise the different categories of such harms and links them to current theories on surveillance on the one hand and on possible design measures on the other.

Keywords

Chilling Effect, Contextual Integrity, Data Mining, Minimum Harm by Design, Discrimination, Privacy, Privacy by Design, Social Sorting, Surveillance.

1. Introduction

PbD is a framework that aims to embed privacy protection into the development of technologies starting from its earliest phases.[1] One of the core assumptions of PbD is the 'win-win' principle,

[1] Ann Cavoukian, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era', in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, ed. George O.M. Yee (Hershey: Information Science Reference, 2012), 170–207.

according to which there is no trade-off between privacy and security. By applying the PbD framework, it is indeed supposedly possible to have both.[2]

The framework as such consists of seven foundational principles that describe the basic ideas and concepts of PbD on an abstract level. Beyond the aforementioned win-win thesis, these principles express the idea that privacy-protecting measures should be taken preventively ('proactive not reactive; preventive not remedial'), operated as default rules and embedded into the design of technologies ('privacy as the default setting' and 'privacy embedded into design'), instead of being adopted as late remedies once privacy violations have already occurred. Moreover, the PbD principles prescribe that the adopted measures should address the whole process involving individuals' data, from collection to deletion ('end-to-end security, full lifecycle protection'), implement transparency ('visibility and transparency—keep it open') and give priority to users' interests ('respect for user privacy—keep it user-centric').

However, there are not concrete guidelines on how to put those seven foundational principles into action. This allows for a great variety in the practical applications of the PbD theoretical framework. Such applications have been advanced both by one of the inventors of PbD, Ann Cavoukian,[3] and by other scholars and have led to very different outcomes. While some applications are more sensitive towards companies' interests, others favour individuals' privacy. As examples of the first approach, several suggestions have been made by Cavoukian and her collaborators, who have been very keen on stressing that 'privacy is good for business'.[4] Applications that engage more decidedly with effective privacy protection have been developed

[2] There is an ambiguity regarding the way the win-win principle is understood in the PbD approach. To explain this principle, Cavoukian refers both to the win-win and to the positive-sum paradigm. However, these are two different concepts. We have a win-win situation when, compared to a previous state of affairs, both values (in our case, privacy and security) increase. We have a positive-sum situation when, compared to a previous situation, the *sum* of two values (in our case, the ones assigned to privacy and security) increases. But, unlike the first case, this might also imply that one of the two values decreases, when the other increases enough to maintain the sum of the two values as positive. In other words, we can have a positive-sum scenario also when privacy is sacrificed to a given extent, provided that security increases enough to compensate for this loss. See Christoph Bier et al., 'Enhancing Privacy by Design from a Developer's Perspective', in *Privacy Technologies and Policy*, ed. Bart Preneel and Demosthenes Ikonomou, Lecture Notes in Computer Science 8319 (Berlin Heidelberg: Springer, 2014), 73–85.

[3] On the origins of PbD see Peter Hustinx, 'Privacy by Design: Delivering the Promises.', *Identity in the Information Society* 3, no. 2 (2010): 253–55.

[4] Ann Cavoukian, 'Privacy by Design', 2009, 2, <https://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf>.; Ann Cavoukian and Marilyn Prosch, 'The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users', December 2010, <https://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf>.; Ann Cavoukian and Jeff Jonas, 'Privacy by Design in the Age of Big Data', June 2012, <https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf>.

by the broader engineering community and include, for instance, proposals for electronic petition systems and road tolling systems.[5]

One might say that the label 'PbD' today stands for a variety of applications whose effectiveness in protecting privacy and individuals' interests varies considerably. The most privacy-oriented of such applications demonstrate that it is possible to translate the theoretical model into an effective privacy-protective tool, at least as far as the systems to be designed are not applied to surveillance as their main functionality.[6] Indeed, the effectiveness of PbD—even of its most privacy-oriented applications—seems to be seriously challenged when technologies are deployed for surveillance as their main purpose.

The PbD framework was originally conceived for the business sector as a way to improve consumers' trust through better privacy protection and later expanded to other areas, including public policies.[7] In recent years, in particular, there have been numerous attempts to apply the PbD framework to the security sector and, in particular, to surveillance technologies. Cavoukian herself developed a 'privacy-protective-surveillance' (PPS) system,[8] while in the Eropean Union (EU) there are plans to incorporate the PbD principles in key security actions.

The official commitment of the EU to PbD dates back to 2012, when the European Commission (EC) released a proposal of General Data Protection regulations.[9] Article 23 of this proposal prescribes that individuals and organisations processing personal data should ensure 'data protection by design and by default'.[10] This suggestion was taken up in the final General Data Protection regulation, which was adopted in April 2016.[11] In recent years, the EU increasingly manifested the intention to apply PbD measures to the security domain as well. Two EU

---

[5] Seda Gürses, Carmela Troncoso, and Claudia Diaz, 'Engineering Privacy by Design', in *Conference on Computers, Privacy, and Data Protection (CPDP)*, 2011, https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf; Josep Balasch et al., 'PrETP: Privacy-Preserving Electronic Toll Pricing', in *19TH USENIX SECURITY SYMPOSIUM* (USENIX Association, 2010), 63–78.

[6] Section 3 below clarifies how expressions such as 'technology system with a surveillance functionality' are understood in this paper.

[7] Cavoukian, 'Privacy by Design'.

[8] Ann Cavoukian and Khaled El Emam, 'Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism', September 2013, https://www.ipc.on.ca/images/Resources/pps.pdf.

[9] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 Final.

[10] Although the EU recognises privacy and data protection as two separate rights (s. arts 7 and 8 of the Charter of the Fundamental Rights of the EU), the proposal uses the terms 'privacy by design' and 'data protection by design' as synonyms, s. George Danezis et al., 'Privacy and Data Protection by Design – from Policy to Engineering', Report/Study (ENISA, December 2014), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. For how the two terms are understood in this paper see section 4 below.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 25.

documents, released in 2015, express this trend: the standardisation mandate M530 and the EU Agenda on Security.[12] The former document contains a request by the EC to the EU standardisation bodies to draft a European standard for the management of privacy and data protection, to be applied in the design of security technologies and explicitly refers to the implementation of the PbD approach as the end-goal. The latter document, the EU Agenda on Security, presents PbD as a way to improve EU activity in the security domain, thus also referring to surveillance measures such as the Schengen Information System, the Prüm framework and the Passenger Name Record System. Finally, in April 2016, the EU released Directive 2016/680, which is about the processing of personal data for 'the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[13] For such activities, measures that aim to implement 'data protection by design and by default' must be adopted (art. 20).

The shift in focus towards the security sector represents, in my opinion, a critical turn. My thesis claims that a meaningful and effective mitigation of the potential harms of surveillance requires a substantial revision of the PbD framework. As I will argue extensively, a key functionality of surveillance uses of technologies is to influence individuals' behaviour, choices and chances. Surveillance is, therefore, very likely to clash not only with privacy but also with other values of critical importance to the EU, such as the freedom of thought, conscience and religion, the freedom of expression and information, the freedom of assembly and association, the principle of non-discrimination and the principle of equality between men and women.[14] For now, I will refer to these additional categories as the social and political harms of surveillance.

In section 2 I clarify what I mean by 'surveillance' and identify theories of surveillance that in my view enable us to identify the mechanisms leading to the social and political harms of surveillance. Although it draws extensively on existing literature, this section is not meant to provide a comprehensive overview of surveillance theories. Section 3 addresses the question of how it is possible to distinguish 'surveillance technologies' from other technologies and

[12] Commission Implementing Decision of 20.1.2015 on a Standardisation Request to the European Standardisation Organisations as Regards European Standards and European Standardisation Deliverables for Privacy and Personal Data Protection Management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council, M530, C(2015) 102 Final and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security, COM(2015) 185 Final.

[13] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[14] See arts. 10, 11, 12, 21 and 23 of the Charter of Fundamental Rights of the EU. The list of values is not meant to be exhaustive.

suggests adopting the expression 'surveillance uses of technologies' for the former. Section 4 is committed to identifying a conceptualisation of privacy that is suitable to effectively address privacy violations caused by surveillance, including the ones that are not recognised as such in the PbD framework. Section 5 explains why surveillance technologies deserve special consideration and what the shortcomings of the PbD framework are when applied to surveillance. In section 6, I discuss current approaches that attempt to conceptualise a broader range of the harms of surveillance than current policy practices. While I share most of the assumptions of these theories, I opt for a different strategy to address the harms of surveillance and suggest a different categorisation of them. In section 7, I attempt to articulate the connection between the theories of surveillance illustrated in section 2, the harms of surveillance that go beyond privacy violations and possible mitigation strategies at the design level. I suggest reworking the PbD framework in an approach that can be called 'Minimum Harm by Design' (MHbD), in which the main feature consists of aiming to comprehensively address the negative effects of surveillance instead of focussing solely on privacy.[15] Section 8 concludes by highlighting the advantages and limitations of the proposed framework and pointing at possible trajectories of future research.

2. Contemporary surveillance: Classify, predict, exclude

Surveillance and privacy are the most disputed concepts in contemporary research. Although there seems to be consensus on the idea that privacy is (at least to a given extent) something worth preserving and that surveillance might carry risks that should be addressed, a univocal, generally accepted definition of these two concepts is still unavailable.[16] Considered in the light of the proliferation of surveillance techniques in our world, such a state is something of a paradox: the more we are affected by surveillance, the less it seems possible to come up with a clear definition. As Kevin Haggerty and Richard Ericson argued, 'while surveillance is now ubiquitous, it is also diverse, multi-faced, and employed in such a panoply of projects that it is almost impossible to speak coherently about "surveillance" more generally'.[17]

[15] Footnote deleted for blind-review purposes.

[16] On the difficulty of defining privacy and surveillance see, for instance, Daniel J. Solove, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* 154, no. 3 (January 1, 2006): 477–564, doi:10.2307/40041279 and Kevin D. Haggerty and Richard V. Ericson, 'The New Politics of Surveillance and Visibility', in *The New Politics of Surveillance and Visibility*, ed. Kevin D. Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2007), 3–25.

[17] Kevin D. Haggerty and Richard V. Ericson, 'The New Politics of Surveillance and Visibility', in *The New Politics of Surveillance and Visibility*, ed. Kevin D. Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2007), 22.

Accordingly, this paper will not try to put forward a comprehensive definition of surveillance, nor will it try to provide an overview of existing surveillance theories.[18] Rather, it will focus on a few ways of understanding surveillance that are relevant in the context of the present discussion. In order not to digress, the discussion is inevitably selective: not only does it not consider interpretations pertaining to forms of sous-veillance,[19] surveillance as care,[20] or surveillance as participation,[21] it also admittedly avoids engaging with authors such as Gilles Deleuze, Bruno Latour and Shoshana Zuboff,[22] since their theories, although very influential in contemporary surveillance studies, are not immediately relevant for the purposes of this paper.

A first interpretation of surveillance relevant to the present discussion is Michel Foucault's well-known metaphor of the Panopticon. In the Panopticon, the circular building designed by Jeremy Bentham, inmates are constantly visible. They never know whether they are surveilled at a certain moment, but they know that *they always might be*: power is, at the same time, 'visible and unverifiable'.[23] As a result, inmates internalise power and behave according to the rules, even when no actual surveillance is taking place at a particular moment. The main function of this form of surveillance is to discipline: it is meant to obtain a certain kind of behaviour on the side of the inmates and it also operates independently of any particular information gained about individuals.

Understandings of surveillance based on the Panopticon metaphor have been criticised as not being able to capture the specificity of contemporary surveillance.[24] Discipline, it is argued, is not the major function of surveillance nowadays. Rather, today's surveillance can be better

---

[18] For a recent attempt to map surveillance theories comprehensively, see Maša Galič, Tjerk Timan, and Bert-Jaap Koops, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation', *Philosophy & Technology*, 13 May 2016, 1–29, doi:10.1007/s13347-016-0219-1.

[19] Steve Mann, Jason Nolan and Barry Wellman, 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments.', *Surveillance & Society* 1, no. 3 (1 September 2002): 331–55.

[20] James P. Walsh, 'From Border Control to Border Care: The Political and Ethical Potential of Surveillance', *Surveillance & Society* 8, no. 2 (18 December 2010): 113–30; Alison Marie Kenner, 'Securing the Elderly Body: Dementia, Surveillance, and the Politics of "Aging in Place"', *Surveillance & Society* 5, no. 3 (1 September 2002): 252–69.

[21] Anders Albrechtslund, 'Online Social Networking as Participatory Surveillance', *First Monday* 13, no. 3 (2008), http://firstmonday.org/ojs/index.php/fm/article/view/2142.

[22] Gilles Deleuze, 'Post-Scriptum Sur Les Sociétés de Contrôle', *L'autre Journal* 1 (1990); Bruno Latour, 'On Recalling ANT', *The Sociological Review* 47, no. S1 (1 May 1999): 15–25, doi:10.1111/j.1467-954X.1999.tb03480.x; Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', Journal of Information Technology 30: 75–89, 4 April 2015, http://papers.ssrn.com/abstract=2594754.

[23] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1979), 201.

[24] See Deleuze, 'Post-Scriptum Sur Les Sociétés de Contrôle' and. Kevin D. Haggerty, 'Tear down the Walls: On Demolishing the Panopticon', in *Theorizing Surveillance : The Panopticon and beyond*, ed. David Lyon (Cullompton: Willan, 2009), 23–45.

defined as 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction' [25] or as 'the collection and analysis of information about populations in order to govern their activities'. [26] According to these definitions, surveillance principally consists of gathering information about individuals in order to assign them to different classes and groups and to treat them differently.

Surveillance in this meaning is nothing new and has been a crucial instrument for states to achieve social control, at least since the affirmation of modern bureaucracy in the 18th century.[27] However, two transformations occurred towards the end of the 20th century that significantly transformed this function of surveillance.

The first change relates to the increasing role played by private actors in performing tasks traditionally carried out by public authorities, such as the provision of health care, education and even internal and external security. Such activities are completed nowadays more and more through public and private partnerships, or are delegated by public authorities to private companies.[28] Moreover, private actors may carry out surveillance activities independently of any public function. Private companies, for instance, routinely surveil consumers for marketing purposes.

To describe this new development of surveillance and drawing on the work of Gilles Deleuze and Felix Guattari,[29] Haggerty and Ericson coined the expression 'surveillant assemblage'.[30] They highlight how contemporary surveillance results from the convergence of disparate systems run by multiple actors: instead of being controlled and coordinated by a central authority (i.e. the state), the different parts of the surveillant assemblage develop separately and are linked to each other through rhizomatic, horizontal connections.

The theorisation of surveillant assemblage also acknowledges the second critical innovation in contemporary surveillance, which refers to the advent of the digital era and to the rapid development of computational techniques, including data mining. In the surveillant assemblage, individuals are separated into a series of pieces of information, then reassembled

---

[25] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2009), 14.

[26] Haggerty and Ericson, 'The New Politics of Surveillance and Visibility', 3.

[27] Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Cambridge: Polity Press, 1990).

[28] On public-private partnerships see also Maria Grazia Porcedda, 'Public-Private Partnerships: A "Soft" Approach to Cybersecurity? Views from the European Union', in *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*, ed. Giampiero Giacomello (New York: Bloomsbury, 2014), 183–211.

[29] Gilles Deleuze, 'Post-scriptum sur les sociétés de contrôle'; Gilles Deleuze, *Foucault* (Frankfurt am Main: Suhrkamp, 2001); Gilles Deleuze and Félix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia* (London: Bloomsbury, 2013).

[30] K. D. Haggerty and R. V. Ericson, 'The Surveillant Assemblage', *The British Journal of Sociology* 51, no. 4 (2000): 605–22.

in a virtual space to give shape to their 'data doubles'. These data doubles circulate in the virtual space, are kept, scrutinised, used for calculations and, even more importantly, 'serve as markers for access to resources, services and power in ways which are often unknown to its referent'.[31] Data mining techniques have enormously expanded the possibilities and the powerfulness of contemporary surveillance, as they allow managing larger amounts of data and processing them in a faster and more sophisticated way. Data mining applications, however, not only have increased the possibility of surveillance activities aimed at classifying and managing individuals and populations. They have also critically moved the focus of surveillance towards prediction. In this perspective, the classification of individuals into groups and the creation of profiles constitute a preliminary step in the process that aims to predict and describe possible futures.[32] Data mining techniques for predictive purposes are typically used, for instance, in hiring processes, when companies want to predict which candidates are more likely to become 'good employees' or by banks that want to establish which customers are more 'creditworthy' (i.e. more likely to pay back their debts in the future or to do so in a way that is more profitable for the bank).[33]

Still understanding surveillance as a set of practices aimed at selecting individuals, Didier Bigo coined the expression 'Ban-opticon' to conceptualise in particular surveillance in the context of global policing. The Ban-opticon retains some aspects of Foucault's theorisation, while combining it with new elements inspired, among others, by Giorgio Agamben's theorisation of the ban.[34] Like Foucault's Panopticon, Bigo's Ban-opticon is not just a description of a building or practice; rather, it points at mechanisms at work in the society at large. However, this conceptualisation does not transpose the Foucauldian model at the global level, arguing that contemporary forms of transnational and global policing are concerned with surveiling everyone. Rather, it maintains that surveillance in this context is concerned with a small number of people who are selected and 'banished', excluded or marked as unwelcome. The Ban-opticon 'excludes certain groups in the name of their future potential behaviour (profiling) and by the way it normalizes the non-excluded through its production of normative imperatives'.[35] The

---

[31] Ibid., 613.

[32] Oscar H. Gandy, 'Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment', in *The New Politics of Surveillance and Visibility*, ed. Kevin D. Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2007), 363–84.

[33] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact', *California Law Review* 104 (14 August 2015), http://papers.ssrn.com/abstract=2477899.

[34] Giorgio Agamben, *Homo Sacer : Sovereign Power and Bare Life*, Meridian, Crossing Aesthetics (Stanford: Stanford University Press, 1998).

[35] Didier Bigo, 'Globalized (In)Security: The Field and the Ban-Opticon', in *Terror, Insecurity and Liberty. Illeberal Practices of Liberal Regimes after 9/11*, ed. Didier Bigo and Anastassia Tsoukala (London: Routledge, 2008), 40.

most important imperative for the normalisation of the majority is, for Bigo, the freedom of movement, as recognised by the EU concerning goods, capitals, information, services and persons.

3. Surveillance uses of technologies

Beyond identifying a theorisation of surveillance that can be usefully put to use, an approach that aims to design a framework to mitigate the negative effects of surveillance through interventions at the technological level (such as the MHbD) is faced with a further challenge: how is it possible to distinguish, in particular cases, a 'surveillance technology' from other technology applications?

This is an arduous task, since technologies are rarely designed and used exclusively for surveillance purposes. Although such technologies certainly exist (for instance, CCTV or body scanners), more often we have to deal with technologies or systems whose principal purpose has nothing to do with surveillance but which can also be used, as a secondary functionality, for surveillance, such as music players. Or we have to deal with technologies that can be used for surveillance as a primary application in some contexts and not in others, such as microphones. Moreover, technologies that are not *per se* surveillance technologies in their actual uses may contribute to surveillance if used in combination with other technologies, or they might become critical to surveillance once they are converted to uses different from their original function. Hence, it seems more appropriate to talk of 'surveillance uses of technologies' than of 'surveillance technologies'. But how is it possible to recognise when a particular technology or system of technologies is deployed for surveillance purposes?

In general, one might say that if a technology application contributes to the realisation of one of the surveillance mechanisms described above (discipline through actual or potential visibility, classification on the basis of collected information, prediction of future behaviour, exclusion of particular groups and normalisation of the majority), it might be considered to be a 'surveillance use of technology'.

To show how such classification can work in practice, I will draw on the example of the public transport system. For the sake of clarity, the example over-simplifies some aspects and is not meant to suggest that the same distinctions will apply in all possible scenarios. It only aims to explain the considerations above and to provide an example to make the MHbD proposal more tangible.

Considering a public transport system, I suggest adopting the following classification, according to which four stages of surveillance-affinity can be identified. At one end of the

spectrum (stage 1), the least surveillance-intensive, we can imagine a free public transport system, for which no tickets are required and no CCTV is installed at stops or on vehicles. In this situation we have a set of technologies (the public transport system) whose primary and unique purpose is to transport people and that does not have any surveillance effect. This does not mean that such a system does not affect peoples' lives, both positively and negatively. The conformation of the transport net, for instance, can facilitate access to employment and to other opportunities for part of the population, while excluding others from such chances. These effects, however, do not appear to be a consequence of surveillance; rather, they seem to be an effect of the very characteristic of the transport system itself and are therefore not relevant to the present discussion.

Consider now that fees are applicable to using public transport. Passengers have to buy a ticket for travelling. This ticket might be, for example, an anonymous, one-way electronic ticket (stage 2). In this case we are dealing with a technology (the ticketing system) whose main functionality is to prove that passengers have paid. However, one could infer from the data saved on the ticket that one person bought it at a specific machine at a certain time and used it to travel from point A to point B at another time. Since, as I assume in this example, these data are stored only on the ticket, are not linked to other data and are not used for further analysis, I consider this form of ticketing system to have a very limited surveillance potential.

Alternatively (stage 3), we can imagine that electronic tickets are not anonymous (for example, because they could only be charged on a personal card) and that these tickets are supported by a technological infrastructure designed to profile passengers' habits for traffic regulation purposes. This might be considered a third stage on our continuum ranging from non-surveillance (uses of) technologies to surveillance (uses of) technologies. Here we have two parallel functionalities for the ticket system: one low-level surveillance functionality, i.e. to provide evidence of payment, and a strong surveillance functionality, i.e. profiling.

Finally (stage 4), we can consider the case of a public transport system that is free for passengers but in which passengers are nevertheless required to validate a personal card upon accessing the public transport. The purpose of the card system is to collect data on individuals for profiling and to deny access to public transport to passengers considered dangerous or undesirable. In this case the exclusive functionality of the card system is surveillance.

I consider the first two stages as scenarios in which technologies are used for non-surveillance purposes, while I suggest the applications in the third and fourth scenarios are 'surveillance uses of technologies'.

For the first two stages, either no harms-minimising measures are necessary (stage 1), or they can be limited to applications inspired by the PbD framework (stage 2). In stage 2, as we have seen, the functionality of the technologies is clearly defined, and the surveillance component is very limited. At this stage, some kind of privacy-protective measures, such as avoiding collection, retention and analysis of data in a central database[36] already apply and seem to be enough to keep the potential harms of surveillance to a minimum. In contrast, the last two stages, as we will see, are the ones that pose major challenges to the PbD model and for which the need for an alternative approach is evident. Technologies aiming at profiling and selecting, as we will see, are not only problematic from a privacy perspective; rather, they can also negatively impact on values directly relevant for society and the political system.

The classification's purpose is to illustrate how the reasoning about particular technology uses can be developed in a given situation, and not to provide a fixed, definitive scheme to be applied as it is for all possible transport systems. The surveillance scale, indeed, makes clear that a particular technology has exclusive surveillance functionality only in a few cases. In most cases, the question about the surveillance-affinity of a technology can be answered only by taking into account both the specific context of its use and the broader context of its interactions with other technologies.

The table below summarises the classifications.

STAGE	TECHNOLOGY SYSTEM	MAIN FUNCTIONALITY/IES	SIDE FUNCTIONALITY	'SURVEILLANCE USE OF TECHNOLOGY'
1	TRANSPORT SYSTEM	TRANSPORT (NON-SURVEILLANCE)	/	NO
2	TICKET SYSTEM	PROOF OF PAYMENT (LOW-LEVEL SURVEILLANCE)	LOCAL (ON THE TICKET) COLLECTION OF FEW, ANONYMOUS, NON-SPECIFIC DATA ON PASSENGERS' MOVEMENTS (LOW-LEVEL SURVEILLANCE)	NO
3	TICKET SYSTEM	PROOF OF PAYMENT (LOW-LEVEL SURVEILLANCE) PROFILING (HIGH-LEVEL SURVEILLANCE)	/	YES
4	PERSONAL CARD SYSTEM	PROFILING (HIGH-LEVEL SURVEILLANCE) SELECTING (HIGH-LEVEL SURVEILLANCE)	/	YES

4. Privacy: Family resemblances and contextual integrity

[36] Balasch et al., 'PrETP'.

If the conceptualisation of surveillance is a challenging task, things do not get easier concerning privacy.

Predominant appraisals of privacy conceptualise it as limited access or as control over access to oneself or one's personal information.[37] Limited access accounts consider privacy to be best protected when a person is beyond the reach of anybody else, and when, as a result, no information about this person is known by others and nobody has physical access to him or her. William Parent's definition of privacy as 'the condition of not having undocumented personal knowledge about one possessed by others'[38] is probably the most influential example of this view. According to Parent, personal information refers to 'facts' about a person that this person does not usually want to be widely known. Privacy involves only 'undocumented' personal information, i.e. information that is not already publicly available. Hence, according to the access account of privacy, we enjoy privacy when nobody accesses information about us that we wish to keep for ourselves or that is available only to a restricted number of people.

Control definitions of privacy move the focus from access to *control* over access: we enjoy privacy when we are able to determine who can have access to information about us and who cannot. Charles Fried provided a classical definition of privacy from this angle. According to him, 'privacy is not simply an absence of information about us in the minds of others; rather, it is the *control* we have over information about ourselves […], is control over knowledge about oneself'.[39]

Such conceptualisations, however, have been criticised for being too centred on the individual and on the notion of separation, and for being inadequate to address the complexity of our interconnected word.[40] As Daniel Solove argued, these accounts reduce privacy to a matter of personal choice, when in fact the question about what information should be protected is determined by what is valued by the society as well.[41] What counts as private, in other words, cannot be established by individuals alone; it is also shaped by social structures and norms. Additionally, limited access and control accounts of privacy are inadequate because many contemporary privacy problems

> involve efforts to gain knowledge about an individual without physically intruding or even gathering data directly from them […], or problems that

[37] Alan Rubel, 'The Particularized Judgment Account of Privacy', *Res Publica* 17 (2011): 275–90.
[38] W. A. Parent, 'Privacy, Morality, and the Law', *Philosophy and Public Affairs* 12 (1983): 269.
[39] Charles Fried, 'Privacy. [A Moral Analysis]', in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984), 209.
[40] Felix Stalder, 'Privacy Is Not the Antidote to Surveillance', *Surveillance & Society* 1 (2009): 120–24.
[41] Daniel J. Solove, 'Conceptualizing Privacy', *California Law Review* 90 (2002): 1087–1155, doi:10.2307/3481326.

> emerge from the way that the data is handled and maintained […], the way it is used […], and the inability of people to participate in its processing […].[42]

Moreover, there are situations in which we not only wish to share our data with others, but also want them to fully control and manage access to such data, like in cases of needed urgent medical treatments.[43]

As a response to these and other shortcomings, conceptualisations of privacy have moved beyond the individualistic understandings and have integrated social and political considerations. For instance, Priscilla Regan has extensively demonstrated that privacy is not only important for individuals, but also serves society's values.[44] In the same vein, other authors have suggested expanding the meaning of privacy to include dimensions that have a more obvious social and political meaning. The proposed additional categories refer, for instance, to privacy of behaviour and action and to privacy of association.[45] These proposals are of central importance for the present papers and will be further discussed in section 6.

These further elaborations and refinements, however, have not led to identifying a generally shared and accepted definition of privacy. Solove's assertion that 'Privacy is a concept in disarray'[46] seems to still be relevant.[47] For the purposes of this paper, however, this lack of clarity does not pose insurmountable problems and can, in my view, be circumvented using two strategies.

The first one is suggested by Solove himself and consists of abandoning the epistemic framework characteristic of most accounts of privacy.[48] These accounts share the effort of identifying some basic characteristics able to capture the common core of all privacy instances. This common denominator for Solove, however, simply does not exist. Rather, privacy can be better conceptualised by relying on Ludwig Wittgenstein's notion of 'family resemblances'. When we talk about privacy in general, we make generalisations about different practices.

---

[42] Daniel J. Solove, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* 154 (2006): 564, doi:10.2307/40041279.

[43] Stalder, 'Privacy Is Not the Antidote to Surveillance.'

[44] Priscilla M. Regan, *Legislating Privacy* (London: University of North Carolina Press, 1995).

[45] Rachel L. Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy', in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2013), 3–32; Charles D. Raab and David Wright, 'Privacy Principles, Risks and Harms', *International Review of Law, Computers & Technology* 28, no. 3 (2014): 277–98. For an overview of positions stressing the social importance of privacy see Charles D. Raab, 'Privacy, Social Values and the Public Interest', ed. Andreas Busch and Jeannette Hofmann, *Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], Politische Vierteljahresschrift*, 46 (2012): 129–51

[46] Solove, 'A Taxonomy of Privacy', 477.

[47] As a further example of recent papers presenting a new conceptualisation of privacy (and one that is different from the recent ones mentioned above), see George E. Panichas, 'An Intrusion Theory of Privacy', *Res Publica* 20, no. 2 (1 May 2014): 145–61.

[48] Solove, 'Conceptualizing Privacy'.

These practices are connected to each other through a net of relationships, although there is no common element shared by all of them. Like the members of a family, the different privacy practices all resemble each other, but not necessarily in the same way. Rather than looking abstractly for the essence of privacy, Solove turns to specific contexts and situations to provide a framework for identifying and recognising privacy issues. He is thus able to identify a set of activities harmful to privacy and to develop a related taxonomy. This taxonomy identifies four groups of activities that potentially harm privacy: information collection, information processing, information dissemination and intrusion.[49] While the first three categories always entail activities regarding personal information, the last one does not necessarily do so.

The second strategy consists of recognising the context-dependency of privacy and making it the keystone of the conceptualisation of privacy. This is the approach adopted by Hellen Nissenbaum in her understanding of privacy as contextual integrity.[50] Nissenbaum focusses on informational privacy, i.e. privacy related to personal information. For her, flows of personal information are regulated by norms that 'prescribe, for a given context, the types of information, the parties who are the subjects of the information as well as those who are sending and receiving it, and the principles under which this information is transmitted'.[51] We enjoy privacy when contextual norms are respected and we speak of privacy violation when contextual norms are breached.

Nissenbaum's framework, compared to the ones criticised by Solove, has two critical advantages. First, it offers a general account of privacy that does not neglect its context-dependency. Second, it acknowledges the social dimension of privacy. Contextual norms, indeed, are specific to each particular society and evolve according to historical, social and geographical conditions. They express, in other words, the 'very fabric of social life' in a given context.[52] Nissenbaum's account, however, also has limitations: for instance, it only focusses on informational privacy, thus omitting privacy violations that do not involve information flows.[53] To discuss whether her framework can be adapted to such cases is beyond the scope

[49] Solove, 'A Taxonomy of Privacy'.
[50] Helen Fay Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, 2010).
[51] Ibid., 141.
[52] Ibid., 3.
[53] On the distinction between privacy and data protection and between the different meanings of privacy, see the Charter of Fundamental Rights of the European Union, 2010/C 83/02 (Arts. 7 and 8), Beate Rössler, 'New Ways of Thinking about Privacy', in *The Oxford Handbook of Political Theory*, ed. John S. Dryzek, 1. publ., The Oxford Handbooks of Political Science (Oxford: Oxford Univ. Press, 2006), 694–712 and Finn, Wright, and Friedewald, 'Seven Types of Privacy'.

of this paper. However, since this paper draws on privacy issues concerning information flows, this limitation will not affect the following discussion.[54]

Solove's taxonomy and Nissenbaum's conceptualisation, thus provide us with a useful basis for identifying privacy issues and harms involved in surveillance activities. For the purposes of the present discussion, I suggest considering a privacy violation taking place when one of the potentially harmful actions individuated by Solove leads to a violation of contextual norms. This is the case, for instance, if data that are collected while I am surfing on the internet (i.e., while ordering plenty of junk-food) are processed to estimate the risk that I suffer or will suffer health diseases and the results are sold to health insurance companies (for instance, in order to calculate a higher health insurance premium). In these examples, an activity identified by Solove as harmful (data processing) leads to a violation of contextual norms in Nissenbaum's understanding, since I do not expect my health insurance to be informed about my purchasing habits by the (online) food store.

5. Shortcomings of PbD applied to surveillance

According to the overview of the different kinds of contemporary surveillance described above, surveillance aims to interfere with individuals' behaviour and opportunities in different ways. These are not necessarily based on the collection of information. Panoptic practices exemplify how surveillance can operate and achieve disciplining effects independent of information collection, while forms of surveillance aimed at classifying individuals, also in their predictive variations, are more dependent on knowledge. However, the information collected and exploited for classifying purposes can be anonymous, and its connection to 'real' individuals does not need to be immediately evident. And yet, all forms of surveillance can have—and indeed *aim to have*—very tangible consequences for 'real' individuals. For instance, anonymous information related to the district of residence might be enough for classification. On the basis of such information, transport owners can then decide to cancel a given line, reducing accessibility to a given district and thereby potentially affecting every one of its residents.

[54] A further limitation of Nissenbaum's approach is the lack of clarity on what characterises a context as such, i.e. on how to distinguish one context from another. This limitation, acknowledged by Nissenbaum, is relevant for the present paper as well, since the MHbD approach relies on Nissenbaum's definition to identify privacy violations. However, I consider this limitation to indicate that Nissenbaum's approach deserves to be further developed and specified (a task that is out of the scope of this paper, but from which the MHbD approach would benefit as well) rather than invalidate the whole framework of privacy as contextual integrity. See Colin J. Bennett, 'Review of Nissenbaum's Privacy in Context', *Surveillance & Society* 8, no. 4 (28 April 2011): 541–43.

This has very important consequences for the suitability of the PbD approach to limit the negative effects of surveillance. Since the collection of information directly related to an identifiable individual is not a necessary element of surveillance, limiting the discourse to privacy violations narrows the focus too much and risks labelling as 'non-harmful' activities that can violate values as important to individuals and society as privacy. Moreover, as we will see shortly, privacy violations occur more often than asserted by Cavoukian.

The shortcomings of the PbD framework applied to surveillance can be illustrated by analysing the proposal of 'privacy-protective-surveillance' (PPS) advanced by Cavoukian and Kahled El Emam.[55] PPS is a specification of the PbD model applied to surveillance and consists of a proposal for improving existing anti-terrorism surveillance in a way that does not intrude on individuals' privacy.

The proposed PPS system is run by government agencies.[56] However, the long-term aim, as we will see below, envisions a close cooperation between the government and private companies. PPS scans the Web and related databases in order to detect evidence of terrorist activities, while using a 'blind-sight' procedure that encrypts personally identifying information (PII). The search is carried out by 'intelligent virtual agents', programmed to detect suspicious activities and flag them. Different virtual agents are designed to search for different activities, for instance, 'buying fertilizer capable of bomb-making' or 'accessing a bomb-making website'. Once an agent detects such an activity, it also accesses the related PII, including name, gender, date of birth, social security number, address etc. This information is encrypted using an encryption key controlled by a court, and no plain-text version is retained. The collected and encrypted personal information, together with information pertaining to the suspected activity, is sent to a central database where it is stored and analysed in order to establish links between different items, i.e. to collate different activities relating to the same individual. Once sets of related items like these are established, probabilistic graphical models are built in order to calculate the likelihood of a terrorist threat. If the estimated probability is high enough, a court warrant is requested to allow the decryption of the related PII and the start of ordinary investigations.

The strength of this proposal, for its advocates, lies primarily in the fact that the data analysis takes place in the encrypted domain, and that the related personal information is disclosed only when the probability of terrorist activities is considered to be high enough and only after a court

[55] Cavoukian and El Emam, 'Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism'.

[56] Cavoukian and El Emam do not specify what kind of agencies would run the system, i.e. intelligence services or the police.

warrant has been issued. Moreover, the fact that the collected PII is encrypted should make over-collection of data unlikely because of the computational costs related to encryption. Cavoukian and El Emam argue that the innocent farmer who buys fertilizer for farming should not be concerned about the search because no personal information on her is disclosed to the authorities. A further advantage in terms of privacy should be assured through a strong involvement of private companies like Google, Facebook and Yahoo. Ideally, in the long term they would perform the search on behalf of the public authorities 'and then turn over to law enforcement a copy of the encrypted files for anonymized analysis … in a privacy-protective manner'.[57]

After closer examination, the optimism of the PPS proponents concerning the privacy protectiveness of PPS is difficult to share. They rely on prevailing definitions of privacy, which, as we have seen, are inadequate to address the challenges to privacy posed by contemporary surveillance practices.[58] For instance, according to understandings of privacy as limited access, no privacy violation occurs in the PPS system because the search performed by the virtual agents does not presuppose access to information that was not already available to the agents before. This is particularly true if, as in the ideal type of PPS, companies like Google, Facebook and Yahoo perform the search themselves. If we turn to accounts of privacy as control over personal information, it seems that the search performed by PPS's virtual agents does not diminish the amount of control of personal information. Indeed, when I write an email, for instance, I entrust a certain amount of personal information to the email service provider, and therefore I am already no longer in control of that information.

In contrast, Nissenbaum's account of privacy as contextual integrity enables us to recognise the privacy violations occurring in the PPS system. Privacy is violated because the transmission principles that regulate communication through the Web are breached. These principles, in fact, restrict the use of my personal information to cases where the information is needed to deliver the requested service, and thus prohibit the service provider from putting it at disposal (or directly using it) for search and analysis for counter-terrorism purposes. In other words, just because the service provider has access to personal information about me that I am no longer in full control of does not entitle the service provider to do whatever it wants with my personal information. When searching (or allowing third parties to search) my email correspondence for suspect activities or contacts, in order to access further personal information related to the targeted activities and to collect this information for further analysis (even if in an encrypted

[57] Ibid., 9.

[58] Cavoukian and El Emam define privacy as 'the ability of individuals to control the collection, use, and disclosure of information about themselves', Ibid., 3.

form), the email service provider is not handling my personal information in the way I expected it to when I entrusted it with my personal data. It is therefore violating the contextual norms regulating the flow of information and—consequently—my privacy.

PPS, moreover, violates privacy in another way. In an advanced stage of the process, as we have seen, the PII related to the identified suspicious activities is encrypted and sent to a central database. Only the PII is encrypted—not the information pertaining to the suspected activities. In the central database, a possible convergence of prior and present evidence pertaining to the same individual is verified (i.e. whether other virtual agents have flagged activities related to the same individual). This analysis, through the linkage of different activities, can lead to re-identification of individuals even when the data have previously been purged from any identifying personal information.

From the discussion of PPS so far we can draw the following conclusion: even if we restrict the focus to privacy violations only, the win-win postulate of the PbD model seems to provide a very thin basis for effectively evaluating surveillance systems. It can easily lead to overlooking privacy violations that are not immediately evident.

The shortcomings of PPS, however, reach further than that. PPS, as I argue, also brings about far-reaching social and political risks. Performing widespread, indiscriminate and continuous surveillance activity is likely to induce panoptic-like self-surveillance or normalisation effects. It is not guaranteed, moreover, that an envisaged court warrant would be an effective protection against the decryption of the selected information. Cavoukian and El Emam do not elaborate on how easy it would be to obtain such a court warrant. However, we have learned from the disclosures about NSA activities that the need of a court warrant per se does not ensure any effective limitation of surveillance and might result in a blanket allowance of surveillance.[59]

Moreover, in the final stage of PPS, as we have seen, probabilistic graphical models are built on the basis of the previous analysis to determine whether the probability of a terrorist threat surpasses a predefined threshold. This kind of predictive surveillance is particularly susceptible to causing discriminatory effects. Statistical models might be very powerful and useful methods to deal with natural threats, for instance, but they are not designed to achieve certainty and to infer fair and exact conclusions about particular cases. A probabilistic process always leads to a certain number of false positives. For example, what if the innocent farmer who, according to

[59] Patrick Toomey and Brett Max Kaufman, 'How Did We Let the NSA Spying Get This Bad?', *The Guardian*, 20 November 2013, http://www.theguardian.com/commentisfree/2013/nov/20/how-nsa-spying-got-this-bad-fisa-secret-court; 'US Foreign Intelligence Court Did Not Deny Any Surveillance Requests Last Year', *The Guardian*, 30 April 2016, http://www.theguardian.com/law/2016/apr/30/fisa-court-foreign-intelligence-surveillance-fbi-nsa-applications.

the PPS advocates, should not be concerned about her privacy, had an email exchange with an acquaintance whose adolescent son now and then looks for 'prohibited' videos on the internet, such as, say, videos on how to build a bomb? Will the probability threshold then be surpassed and our farmer's activity be considered a terrorist threat? Cavoukian and El Emam do not specify the criteria of where to set the threshold. This is, however, a critical point, since the kind of criteria used to establish the probability threshold can contribute to discrimination.

In the next section I will elaborate on these additional risks of surveillance practices and their connection to values and rights protected by the EU Charter of Fundamental Rights.

6. Reworking PbD: Abandon the win-win postulate and broaden the range of harms

In order to overcome the shortcomings of the PbD approach when applied to surveillance, I suggest reworking it according to what can be called the MHbD approach.

The suggested approach abandons the win-win assumption of PbD, while recognising that, as far as surveillance is concerned, harms cannot be completely avoided but can at best be mitigated. Since surveillance includes a series of activities aimed at gaining knowledge over individuals and/or influencing their behaviour and their chances, it is most likely to have a negative impact not only on individuals, but on the social and political system as well. Relying on a win-win assumption might lead to light-heartedly welcoming surveillance measures as harmless when in fact they are not, like in the evaluation of the PPS model described above.[60]

One could say that, while PbD considers a surveillance technology 'privacy-safe until proven dangerous', the MHbD approach considers surveillance systems 'dangerous until proven safe'.[61] The naming of the approach reflects this double shift by substituting 'privacy' with 'minimum harm', whereas the former formulation both expresses the broadening of scope and the minimisation purpose.

The main purpose of MHbD is to recognise and mitigate harms that go beyond privacy violations, i.e. to broaden the scope of PbD to include social and political harms as well.

The need to extend the scope of protections against the possible harms of surveillance has been recognised in recent literature on privacy and surveillance. Charles Raab and David Wright, for instance, have pointed at a limitation of the conventional Privacy Impact Assessment (PIA),

[60] This approach has led some authors to assert that PbD, far from offering concrete ways to overcome the trade-off between privacy and security, just reframes the problem in order to make it more suitable for current policy needs. See Matthias Leese, 'Privacy and Security - On the Evolution of a European Conflict', in *Reforming European Data Protection Law*, ed. Serge Gutwirth, Ronald Leenes, and Paul De Hert, Law, Governance and Technology Series (Dordrecht; Heidelberg: Springer, 2015), 271–89.

[61] Charles D. Raab, 'The Future of Privacy Protection', in *Trust and Crime in Information Societies*, ed. Robin Mansell and Brian Collins (Cheltenham: Edward Elgar, 2005), 282–318, as referred in Raab and Wright, 'Privacy Principles, Risks and Harms', 16.

which solely focusses on the privacy of the individual, thus neglecting to address the risks posed by surveillance to other values.[62] They suggest expanding the scope of the impacts to be assessed and to consider the conventional PIA as constituting the inner circle of a series of four cumulative circles, whose scope progressively expands. The second, broader circle, which they call 'PIA_2', focusses on the individual's social and political relationships, including freedom of speech and association. Harms to this second circle include, for instance, the chilling effect. The third circle, 'PIA_3', is concerned with the impact of surveillance on the groups and categories to which individuals belong or are assigned by others. It focusses specifically on surveillance activities that profile and classify, which are likely to negate the principles of equality and non-discrimination. The broader circle, PIA_4, considers the impact of surveillance on society and the political system as a whole and its consequences on citizenship and the relations of the individual with the state and other organisations.

According to Raab and Wright, the limitations of conventional PIA are not due to an intrinsic limitation of the privacy concept; rather, they derive from a too narrow focus on one of its aspects, i.e. information privacy: 'it is not that "privacy" is too narrow or impotent to contend with contemporary infringements of rights, but that information privacy and the array of principles designed specifically for its protection might be too limited for this contention'.[63] Because data protection is a kind of privacy that puts the individual in the foreground more than other types, the contemporary focus on data protection prevents addressing privacy-related issues with a more marked social and political character.

In order to overcome these shortcomings, the authors suggest distinguishing seven types of privacy by adding to Roger Clarke's four categories (privacy of personal information, privacy of the person, privacy of personal behaviour and privacy of personal communication) three additional categories: privacy of location and space, privacy of thoughts and feelings and privacy of association.[64] In particular, privacy of thoughts and feelings and privacy of association have a clearly recognisable political value: they aim to prevent the government from knowing political dispositions that individuals do not want to disclose, and they should protect individuals' freedom to associate with others without being monitored. Focussing on these additional categories of privacy allows formulating further privacy principles such as, to name

[62] Charles D. Raab and David Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment', in *Privacy Impact Assessment*, ed. David Wright and Paul De Hert (Dordrecht: Springer, 2012), 363–83.
[63] Raab and Wright, 'Privacy Principles, Risks and Harms', 2.
[64] Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', 1997, http://www.rogerclarke.com/DV/Intro.html. See also; Finn, Wright, and Friedewald, 'Seven Types of Privacy'.

but a few, the right to dignity, the right to autonomy, the right to assemble and associate with others.

The suggested MHbD approach shares with Raab's and Wright's proposal the point of departure, i.e. the idea that the debate on the impact of surveillance needs a broader focus. Moreover, the two approaches converge on the idea that rights, values and harms can be linked to each other. As Raab and Wright write: 'some privacy rights can also function as privacy principles that can be used for identifying risks and harms',[65] whereas principles are defined as 'shared values'.[66]

However, MHbD also differs from Raab's and Wright's proposal in three ways.

The first aspect concerns the relationship between the MHbD approach and PIA. PIA has been defined as 'a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts'.[67] A PIA, in order to be effective, should be carried out as early as possible and should be carried on also after the technologies at stake have been introduced and applied. The focus of the MHbD approach, on the other hand, is specifically on the design phase of a technology or a system. However, in order to identify which design measures should be implemented, MHbD is also concerned with a sort of preliminary assessment of which harms can be brought about by the adoption of a given technology. Since, however, MHbD necessarily intervenes at a stage in which the technology (system) has not been developed yet, the sort of assessment to be carried out has a more theoretical character. This is why it is necessary to make explicit the connections between the functions of surveillance as they have been highlighted in the literature and their possible harms—a task that will be addressed in the next section.

Second, the MHbD proposal differs from Raab's and Wright's suggestion as the strategy adopted in order to broaden the scope of the harms considered. While Raab and Wright opt to expand the meaning of privacy, I suggest focussing on the political and social harms of surveillance independent of their possible connection to (previous) privacy violations. I recognise that Raab's and Wright's approach may have strategic advantages, such as potentially

---

[65] Raab and Wright, 'Privacy Principles, Risks and Harms', 8.

[66] Ibid. Given this connection, the paper also does not consider rights-based and harms-based approaches to regulatory policies as being opposed to each other. For a view contrasting the two approaches see Finn, Wright, and Friedewald, 'Seven Types of Privacy' and Raab and Wright, 'Privacy Principles, Risks and Harms'.

[67] Paul De Hert and David Wright, 'Introduction to Privacy Impact Assessment', in *Privacy Impact Assessment*, ed. David Wright and Paul De Hert (Dordrecht ; Heidelberg: Springer, 2012), 5.

extending the protection offered by existing privacy law. However, in my opinion, this approach also has drawbacks. Although it is broadly acknowledged that privacy is not a one-dimensional concept, the actual belonging to privacy of some of the categories that the two authors bring under its umbrella is controversial. For instance, it is difficult to see why the seventh type of privacy mentioned above (privacy of assembly), should be considered a form of privacy, instead of sticking to its conventional standing as a distinct right that has for a long time been recognised and protected independently of its connection to privacy. Moreover, the inclusion into the meaning of privacy of other categories, such as privacy of location and privacy of thoughts and feelings, does not really make the connection to the political and social harms of surveillance more straightforward. To make this connection explicit, the authors have to refer to privacy principles, which, again, appear to be better protected through their connection to other rights. Examples of such principles are the freedom of thought and the right to assemble and associate with others. By conceiving privacy so broadly, Raab's and Wright's approach risks, in my opinion, making the concept of privacy unrecognisable or, worse, to make it appear a vague, derivative and redundant concept.[68] In the words of Daniel Solove, it might strengthen the impression that 'Privacy seems to be about everything, and therefore it appears to be nothing'.[69]

The third aspect that differentiates MHbD and PIA is the way they define the categories of the additional harms of surveillance. As we have seen, Raab and Wright identify four concentric circles that focus respectively on the harms of surveillance to individual privacy (PIA_1), the individual's 'social and political relationships and her relative position within society and the market' (PIA_2), the groups and categories to which individuals belong or are assigned (PIA_3) and society and the political system (PIA_4). MHbD, in contrast, identifies three domains of harms, whose overall scope overlaps with the four PIA circles but categorises them differently. The first domain includes harms to privacy, understood as being broader than information privacy only, but also narrower than how Raab and Wright suggest. For instance, it includes the respect for private and family life and the protection of personal data, but it does not include privacy of assembly.[70] The second domain concerns harms that affect the constitution of society. I consider most of the principles listed under the chapters 'equality' and 'solidarity' of the EU Charter of Fundamental Rights to be indicators of a relatively equal society and to

[68] For an early criticism in this direction see Judith Jarvis Thomson, 'The Right to Privacy', *Philosophy & Public Affairs* 4 (1975): 295–314.

[69] Solove, 'A Taxonomy of Privacy', 479.

[70] I am aware that a specification of which aspects exactly I consider belong to privacy would be advantageous here. This is, however, a task for another day, since to discuss it in this paper would bring us too far from its focus.

consider the value ultimately protected by them to be social justice. This domain includes, for instance, the principles of non-discrimination, equality between men and women, access to social security and social assistance, and access to health care. Discrimination, based on gender and race, for instance, but also on social status, familiar economic background etc. impact this second sphere negatively. The third sphere focusses on the harms affecting the political constitution. Some of the principles stated by the EU Charter of Fundamental Rights under the chapter 'freedoms' can be considered indicators of a political constitution that protects individual freedom and enables citizens' participation in the political sphere. Because individual freedoms and participation are essential for the flourishing of democracy, democracy can be considered the value ultimately protected by such principles. These principles include, for instance, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom of assembly and of association. As exemplar of the consequences of surveillance having a negative impact on this domain of principles, the chilling effect can be named. In both domains, the negative effects of surveillance impact the social and political constitution in a substantial way rather than in a formal one: i.e. they do not affect the formal entitlement individuals have on the mentioned rights, but *de facto* prevent them from (fully) enjoying these rights. The lists of principles and possible harms are not meant to be exhaustive. Rather, they provide a sort of basic systematisation, or a template, which can be filled with more principles (not necessarily already recognised as rights) and possible harms. Although the identified domains (referring to the social or political basic organisation of a society) surely interact with each other, I consider them to be more sharply circumscribed than the ones identified by Raab and Wright. Indeed, as we have seen, the classification proposed in the MHbD at least partially corresponds to the structure of the EU Charter of Fundamental Rights.

7. MHbD: Linking surveillance mechanisms, values and harms

As anticipated above, in order to anticipate which harms a surveillance use of technology can bring about and intervene at the design level, the MHbD approach should provide guidelines to link the planned surveillance functionality with the possible or expected harms.

Regarding privacy, the mechanisms leading to its violation have been highlighted extensively, and a wide range of privacy-preserving techniques has been developed, including strategies to avoid collection, retention and analysis of data in a central database.[71] In contrast, while the social and political negative effects of surveillance are widely recognised, the mechanisms

[71] See for instance Solove, 'A Taxonomy of Privacy' and Balasch et al., 'PrETP'.

leading to them and the corresponding mitigating design measures have been relatively less explored.

The following discussion, therefore, will focus on the classes of harms affecting the social and political domain and the corresponding mitigation measures. For each class, the discussion will focus on a kind of harm that can be considered a typical example, namely, discrimination for social effects and the chilling effect for political effects.

What are, then, the mechanisms leading to the harms labelled above as pertaining to the 'social consititution'? The social negative effects of surveillance are linked to the forms of surveillance described in section 2 that aim to classify people into different groups in order to treat them differently. This critical function of surveillance has been labelled by David Lyon as 'social sorting'.[72] Social sorting can lead to discrimination, i.e. by denying to some social groups access to basic services. Critical for the discriminatory potential of this form of surveillance is the fact that the classification of persons into different groups results not only from individual characteristics, but on the basis of pre-existing classifications and assumptions as well.[73] As stressed by Oscar Gandy, personal 'profiles are fundamentally relational, or comparative, rather than *individual* identities'.[74] For instance, the best candidates for a new position are selected not only on the basis of their personal characteristics and qualification, but also on the basis of assumptions made about the class of people (male vs female, native vs non-native etc.) they are assigned to.[75] This makes apparent how pre-existent discriminatory patterns can easily flow into social sorting techniques and be perpetuated and reinforced, even if the programmers did not consciously aim to design a discriminatory system.

The mechanisms that lead to discrimination in data mining, indeed, are subtle and multiple. It is not even necessary for discrimination to occur to rely on sensitive personal information, such as that pertaining to gender, ethnicity, political orientation etc… This sort of information, indeed, can be easily substituted by data that do not directly relate to sensitive attributes, but are good indicators for them, such as being a homeowner for age or the district of residence for ethnicity.[76] Moreover, discriminatory effects can arise from pre-existing biases in the datasets, or they can occur at any of the further stages of data mining, for instance, while defining the

---

[72] David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London: Routledge, 2003).

[73] Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, Colo: Westview Press, 1993); Oscar H. Gandy, *Coming to Terms with Chance : Engaging Rational Discrimination and Cumulative Disadvantage* (Farnham: Ashgate, 2009).

[74] Gandy, 'Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment', 370.

[75] Barocas and Selbst, 'Big Data's Disparate Impact'.

[76] Faisal Kamiran, Toon Calders, and Mykola Pechenizkiy, 'Techniques for Discrimination-Free Predictive Models', in *Discrimination and Privacy in the Information Society: Data Mining and Profiling Large Databases*, ed. Bart Custers et al. (Berlin, Heidelberg: Springer, 2013), 223–41.

groups in which individuals should be classified or while constructing the algorithms that should assign different values to different characteristics.

Which design solutions are then meaningful to minimise such effects?

Even if they cannot eliminate the risk of discrimination, measures such as reducing the overall amount of data collected and deleting any sensitive information can be a first step to mitigate discrimination.

Further, more elaborate technical solutions address the different stages of data mining processes, from the use of the available datasets to the programming of the algorithms and the evaluation of the results.[77] Measures that aim to remove the biases inherent to the available dataset consist in changing the class labels from the data that are used for constructing the 'groups' that will serve as the basis for future classifications ('massaging'). Or they can consist of assigning different weights to attributes of the existing data sets ('reweighing'), or the dataset can be re-sampled in a discrimination-free way ('sampling'). A second set of strategies focusses on the algorithms used for assigning or predicting class memberships. Examples of these interventions consist in privileging algorithms that are less precise in distinguishing on the basis of sensitive attributes and are known as 'discrimination-aware decision tree introduction'. Finally, a further cluster of measures focusses on the results of predictive data mining and consists in merging the generated profiles into larger and less discriminative groups. This method is called 'decision tree leaf relabeling'.[78]

As to the effects that are relevant from a political point of view, I suggest relating the mechanisms behind them to the normalising power of surveillance I discussed in section 2. Bigo's conceptualisation, in particular, showed that although contemporary surveillance practices focus on excluding minority groups, they have at the same time normalising effects on the majority of people. As we have seen, Bigo mentions as normalising mechanism the imperative of mobility, which does not seem to be relevant for the chilling effect. Although, I argue, this focus on mobility derives from Bigo's concentration on new forms of policing and, in particular, with the ones concerned with border controls, management of migration flows and the profiling of individuals considered to be dangerous. I suggest considering the normalisation effects highlighted by Bigo as being generalizable to other domains as well. In order not to attract unwanted attention from the surveilling agencies, for instance, individuals may be induced to avoid conspicuous behaviours, conform to mainstream opinions, or to

[77] Ibid.

[78] For more details on these techniques see Ibid. and the further contributions on the topic in Bart Custers et al., eds., *Discrimination and Privacy in the Information Society: Data Mining and Profiling Large Databases* (Berlin, Heidelberg: Springer, 2013).

positions that accommodate the government's official policy, or to renounce or openly express their dissent.[79] Such phenomena, known as the chilling effect, can at least partially inhibit individuals from exercising fundamental rights such as freedom of information, freedom of religion, freedom of speech, freedom of the press and peaceful assembly.

What are, then, the mechanisms that lead to this normalisation effect? They might be traced back to the feeling of being potentially constantly under surveillance, without being able to know if this is actually the case. Although, as we have seen, the Panopticon as an explanatory metaphor does not suit contemporary surveillance, not all of Foucault's explanation of panoptical power must be rejected. I maintain, in contrast, that what he saw as the main strength of panoptical surveillance still applies to some contemporary surveillance practices. This strength resides in the visibility and non-verifiability of surveillance: the surveilled are aware of the existence of a surveillance system that is potentially constantly at work, but they can never verify whether in a given moment the system is actually operating, nor if they are actually targeted by it.

If this interpretation holds, then, the way to minimise the chilling effect of a given surveillance system is either to reduce its visibility, or to make it verifiable (or both). I consider the first option to be undesirable, however, since it would just render surveillance activities secret, thereby undermining democratic control. The second option, increasing verifiability of the surveillance measures, seems more promising. It should, in other words, be possible for people to verify when and under which circumstances they are under surveillance (and when not). This would not eliminate the chilling effect completely, but it would at least weaken the 'vague feeling of surveillance'[80] that seems to be at the basis of the chilling effect.

To transpose such principle into practice and into design measures is a particularly challenging task, and one that would require consistent further engineering research, which is out of the scope of this paper.[81] However, it is possible to give an idea of what should be achieved through such measures by referring to the transport example introduced in section 3. In stage 3 of the proposed classification, for instance, passengers are requested to buy non-anonymous electronic tickets connected to a personal card whose data are used for profiling purposes. In order to address the harms caused by the chilling effect, public transport users can be supplied

[79] Maria Los, 'Looking into the Future: Surveillance, Globalization and the Totalitarian Potential', in *Theorizing Surveillance: The Panopticon and beyond*, ed. David Lyon (Cullompton: Willan, 2009), 69–94.
[80] 'Opinion of Advocate General Cruz Villalón, Case C-293/12, Digital Rights Ireland, 12.12.2013', §52.
[81] Part of these measures would overlap with ones increasing transparency. On the challenges to enhance transparency through design measures see Tal Zarsky, 'Transparency in Data Mining: From Theory to Practice', in *Discrimination and Privacy in the Information Society: Data Mining and Profiling Large Databases*, ed. Bart Custers et al. (Berlin, Heidelberg: Springer, 2013), 301–24.

with devices that enable them to verify whether and when data on them have been collected. This only makes sense, obviously, if the collection of data is exclusively activated when actual information on a particular line is needed and not by default, on all means of public transport. Furthermore, it could be useful to clearly state for which kind of profiling the data are collected. If the aim of profiling is to improve traffic regulation, then only the data strictly necessary for this regulation should be collected.

The table below summarises the link between the mechanisms of surveillance that can lead to harms, the harms and the domains, values and principles negatively affected by them. None of its categories is meant to be exhaustive. Rather, they are considered a first step towards a systematisation that will surely benefit from specification or even amendment through further research.

Domain	Values	Related rights and principles	Harmful surveillance functions	Elements leading to harms	Harms	Design mitigation strategies
Social	Equality Solidarity Social justice	Non discrimination Equality between men and women Access to social security and social assistance Access to health care	Classification Social sorting	Large amounts of data available Sensitivity of data Biases in the datasets Use of discriminative algorithms	Discrimination	Minimisation of data collection Deletion of sensitive attributes Remove biases from data sets Programme discriminatory-aware algorithms Relabel profile outcomes
Political	Freedom Participation Democracy	Freedom of thought, conscience and religion Freedom of assembly and association	Exclusion / Normalisation	Visibility and non-verifiability of Surveillance	Chilling effect	Enable visibility of surveillance coupled with verifiability

8. Summary, limitations of the proposed approach and outlook

In this paper, I have put forward the MHbD approach, a proposal to overcome the shortcomings of PbD when applied to surveillance.

MHbD differs from PbD in two critical ways. First, it acknowledges that the possible harms of surveillance go beyond privacy violations only and attempts to provide guidelines to address them. Second, it abandons the win-win principle of PbD and shifts the burden of the proof on the parties administering surveillance.

This has two advantages compared to PbD. First, it allows us to more broadly assess the potential harms of surveillance, including harms that would not be recognised as such according to the PbD framework. Second, it puts surveillance measures under a more rigourous scrutiny than PbD as far as privacy violations are concerned. Overall, it can be expected to offer a better protection against the risks of surveillance than PbD.

Regarding the task of broadening the scope of the considered harms, the main contribution of the MHbD approach, as I see it, consists in a systematisation effort. It provides a sort of template that systematises the different categories of surveillance harms and links them to current theories on surveillance on the one hand and on possible design measures on the other.

Admittedly, MHbD also has limitations. It aims, in the end, to enable identifying technical solutions to mitigate the harms of surveillance. However, this is a task that cannot be demanded only to technical solutions. On the one hand, the broader legal, political, social and moral context is critical for both identifying what kinds of harms should be more urgently addressed and for providing a framework to decide what counts as political and social harms. On the other hand, technical solutions should also be backed up by legal and policy instruments in order to be effective. Technical interventions aimed at making surveillance systems more visible and verifiable, for instance, can have no positive effects if they are not supported by external structures that make accountability enforceable.[82] Moreover, the application of mitigating techniques *per se* do not make a particular surveillance measure acceptable or legitimate. Indeed, the harms can be considered still too significant and therefore unacceptable. Also in this case, the decisive criteria are of a political, legal and ethical nature and, as such, they are

[82] Discussing accountability and oversight mechanisms for surveillance technologies is out of the scope of this paper. For recent developments in the EU legal framework and an account of existing frameworks see, respectively, Fanny Coudert, 'Accountable Surveillance Practices: Is the EU Moving in the Right Direction?', in *Privacy Technologies and Policy*, Proceedings of the Second Annual Privacy Forum, APF 2014 (Cham: Springer, 2014), 70–85 and Zhendong Ma et al., 'Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems', in *Privacy Technologies and Policy*, Proceedings of the Second Annual Privacy Forum, APF 2014 (Cham: Springer, 2014), 101–16.

context dependent and subject to negotiation and revision. But, as necessary as these external measures are, the reference to them is also inherently ambiguous, since law, policy, morality and society can act at the same time as legitimising forces for harmful surveillance measures and as sources of contestation for them.

Notwithstanding these limitations, the MHbD approach can, in my view, contribute to overcoming some shortcomings of current theories and policies. If the PbD model in its current version becomes the standard way of evaluating surveillance practices in Europe, it will be difficult to make the case for also focussing on the social and political risks of surveillance, because they simply do not fit the PbD paradigm. It is therefore critical that alternative models are available that also stress the importance of the potential negative effects of surveillance beyond privacy.

Moreover, by stressing the importance of looking directly at the social and political dimension of surveillance, the theoretical framework put forth in this paper might encourage further research in this direction both in the field of humanities and from an engineering perspective. From the former perspective, it might enable the identification of further social and political effects of surveillance that are still in the shadow of privacy. From an engineering perspective, this new path could lead to creative and innovative technical solutions that are left unexplored now by a research focus too centred on privacy.

Acknowledgments

Deleted for blind-review

Bibliography

Agamben, Giorgio. *Homo Sacer : Sovereign Power and Bare Life*. Stanford.: Stanford Univ. Press, 1998.

Albrechtslund, Anders. 'Online Social Networking as Participatory Surveillance'. *First Monday* 13, no. 3 (2008). http://firstmonday.org/ojs/index.php/fm/article/view/2142.

Balasch, Josep, Alfredo Rial, Carmela Troncoso, Christophe Geuens, Bart Preneel, and Ingrid Verbauwhede. 'PrETP: Privacy-Preserving Electronic Toll Pricing', In *19TH USENIX SECURITY SYMPOSIUM*, 63–78. USENIX Association, 2010.

Barocas, Solon, and Andrew D. Selbst, 'Big Data's Disparate Impact'. *California Law Review* 104 (August 14, 2015), http://papers.ssrn.com/abstract=2477899. Accessed March 24, 2016.

Bennett, Colin J. 'Review of Nissenbaum's Privacy in Context'. *Surveillance & Society* 8, no. 4 (April 28, 2011): 541–43.

Bier, Christoph, Pascal Birnstill, Erik Krempel, Hauke Vagts, and Jürgen Beyerer. 'Enhancing Privacy by Design from a Developer's Perspective'. In *Privacy Technologies and Policy*, edited by Bart Preneel and Demosthenes Ikonomou, 73–85. Lecture Notes in Computer Science 8319. Berlin Heidelberg: Springer, 2014.

Bigo, Didier. 'Globalized (In)Security: The Field and the Ban-Opticon'. In *Terror, Insecurity and Liberty. Illeberal Practices of Liberal Regimes after 9/11*, edited by Didier Bigo and Anastassia Tsoukala, 10–48. London and New York: Routledge, 2008.

Cavoukian, Ann. 'Privacy by Design'. 2009.

https://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf. Accessed March 24, 2016.
———. 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era'. In *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, edited by George O.M. Yee, 170–207. Hershey: Information Science Reference, 2012.
Cavoukian, Ann, and Khaled El Emam. 'Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism', September 2013. https://www.ipc.on.ca/images/Resources/pps.pdf. Accessed March 24, 2016.
Cavoukian, Ann, and Jeff Jonas. 'Privacy by Design in the Age of Big Data', June 2012. https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf. Accessed March 24, 2016.
Cavoukian, Ann, and Marilyn Prosch. 'The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users', December 2010. https://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf. Accessed March 24, 2016.
Clarke, Roger. 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', 1997. http://www.rogerclarke.com/DV/Intro.html.
Coudert, Fanny. 'Accountable Surveillance Practices: Is the EU Moving in the Right Direction?' In *Privacy Technologies and Policy*, 70–85. Proceedings of the Second Annual Privacy Forum, APF 2014. Cham: Springer, 2014.
Custers, Bart, Toon Calders, Bart Schermer, and Tal Zarsky, eds. *Discrimination and Privacy in the Information Society: Data Mining and Profiling Large Databases*. Berlin, Heidelberg: Springer, 2013.
Dandeker, Christopher. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Cambridge: Polity Press, 1990.
Danezis, George, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, and Stefan Schiffner. 'Privacy and Data Protection by Design—from Policy to Engineering'. Report/Study. ENISA, December 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.
De Hert, Paul, and David Wright. 'Introduction to Privacy Impact Assessment'. In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 3–32. Dordrecht; Heidelberg: Springer, 2012.
Deleuze, Gilles. *Foucault*. Frankfurt am Main: Suhrkamp, 2001.
———. 'Post-scriptum sur les sociétés de contrôle'. *L'autre Journal* 1 (1990).
Deleuze, Gilles, and Félix Guattari. *A Thousand Plateaus: Capitalism and Schizophrenia*. London: Bloomsbury, 2013.
Finn, Rachel L., David Wright, and Michael Friedewald. 'Seven Types of Privacy'. In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet, 3–32. Dordrecht: Springer, 2013.
Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, Alexander Street Press, 1979.
Fried, Charles. 'Privacy. [A Moral Analysis]'. In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, 203–22. Cambridge: Cambridge University Press, 1984.
Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation'. *Philosophy & Technology*, May 13, 2016, 1–29. doi:10.1007/s13347-016-0219-1.
Gandy, Oscar H. *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Farnham: Ashgate, 2009.
———. 'Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment'. In *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson, 363–84. Toronto: University of Toronto Press, 2007.
———. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview Press, 1993.
Gürses, Seda, Carmela Troncoso, and Claudia Diaz. 'Engineering Privacy by Design', paper presented at the *Conference on Computers, Privacy, and Data Protection (CPDP)*, 2011. https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf. Accessed March 24, 2016.
Haggerty, K. D., and R. V. Ericson. 'The Surveillant Assemblage'. *The British Journal of Sociology*

51 (2000): 605–22.
Haggerty, Kevin D. ‘Tear down the Walls: On Demolishing the Panopticon’. In *Theorizing Surveillance : The Panopticon and beyond*, edited by David Lyon, 23–45. Cullompton: Willan, 2009.
Haggerty, Kevin D., and Richard V. Ericson. ‘The New Politics of Surveillance and Visibility’. In *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson, 3–25. Toronto: University of Toronto Press, 2007.
Hustinx, Peter. ‘Privacy by Design: Delivering the Promises.’ *Identity in the Information Society* 3, no. 2 (2010): 253–55.
Kamiran, Faisal, Toon Calders, and Mykola Pechenizkiy. ‘Techniques for Discrimination-Free Predictive Models’. In *Discrimination and Privacy in the Information Society: Data Mining and Profiling Large Databases*, edited by Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky, 223–41. Berlin, Heidelberg: Springer, 2013.
Kenner, Alison Marie. ‘Securing the Elderly Body: Dementia, Surveillance, and the Politics of “Aging in Place”’. Surveillance & Society 5, no. 3 (September 1, 2002): 252–69.
Latour, Bruno. ‘On Recalling ANT’. The Sociological Review 47, no. S1 (May 1, 1999): 15–25. doi:10.1111/j.1467-954X.1999.tb03480.x.
Los, Maria. ‘Looking into the Future: Surveillance, Globalization and the Totalitarian Potential’. In *Theorizing Surveillance: The Panopticon and beyond*, edited by David Lyon, 69–94. Cullompton: Willan, 2009.
Lyon, David, ed. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003.
———. *Surveillance Studies: An Overview*. Cambridge: Polity Press, 2009.
Ma, Zhendong, Denis Butin, Francisco Jaime, Fanny Coudert, Antonio Kung, Claire Gayrel, Antonio Mana, et al. ‘Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems’. In *Privacy Technologies and Policy*, 101–16. Proceedings of the Second Annual Privacy Forum, APF 2014. Cham: Springer, 2014.
Mann, Steve, Jason Nolan, and Barry Wellman. ‘Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments.’ *Surveillance & Society* 1, no. 3 (September 1, 2002): 331–55.
Nissenbaum, Helen Fay. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books, 2010.
Panichas, George E. ‘An Intrusion Theory of Privacy’. *Res Publica* 20, no. 2 (May 1, 2014): 145–61.
Porcedda, Maria Grazia. ‘Public-Private Partnerships: A “Soft” Approach to Cybersecurity? Views from the European Union’. In *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*, edited by Giampiero Giacomello, 183–211. New York: Bloomsbury, 2014.
Raab, Charles D. ‘Privacy, Social Values and the Public Interest’. Edited by Andreas Busch and Jeannette Hofmann. *Politik und die Regulierung von Information’ [‘Politics and the Regulation of Information’], Politische Vierteljahresschrift*, 46 (2012): 129–51.
Raab, Charles D. ‘The Future of Privacy Protection’. In *Trust and Crime in Information Societies*, edited by Robin Mansell and Brian Collins, 282–318. Cheltenham: Edward Elgar, 2005.
Raab, Charles D., and David Wright. ‘Privacy Principles, Risks and Harms’. *International Review of Law, Computers & Technology* 28, no. 3 (2014): 277–98.
———. ‘Surveillance: Extending the Limits of Privacy Impact Assessment’, in In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 363–83. Dordrecht; Heidelberg: Springer, 2012.
Regan, Priscilla M. *Legislating Privacy*. London: University of North Carolina Press, 1995.
Rössler, Beate. ‘New Ways of Thinking about Privacy’. In *The Oxford Handbook of Political Theory*, edited by John S. Dryzek, 694–712. Oxford: Oxford University Press, 2006.
Rubel, Alan. ‘The Particularized Judgment Account of Privacy’. *Res Publica* 17 (2011): 275–90.
Solove, Daniel J. ‘A Taxonomy of Privacy’. *University of Pennsylvania Law Review* 154 (2006): 477–564. doi:10.2307/40041279. Accessed March 24, 2016.
———. ‘Conceptualizing Privacy’. *California Law Review* 90 (2002): 1087–1155. doi:10.2307/3481326. Accessed March 24, 2016.
Stalder, Felix. ‘Privacy Is Not the Antidote to Surveillance.’ *Surveillance & Society* 1 (2009): 120–24.
Thomson, Judith Jarvis. ‘The Right to Privacy’. *Philosophy & Public Affairs* 4 (1975): 295–314.

Walsh, James P. ‘From Border Control to Border Care: The Political and Ethical Potential of Surveillance.’ *Surveillance & Society* 8, no. 2 (December 18, 2010): 113–30.
Zarsky, Tal. ‘Transparency in Data Mining: From Theory to Practice’. In *Discrimination and Privacy in the Information Society: Data Mining and Profiling Large Databases*, edited by Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky, 301–24. Berlin, Heidelberg: Springer, 2013.
Zuboff, Shoshana. ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’, Journal of Information Technology 30: 75–89, April 4, 2015. http://papers.ssrn.com/abstract=2594754.