Three Models of Privacy

New Perspectives on Informational Privacy

Jens-Erik Mai

This panel is based on two observations: (i) that digital media are designed such that they track and record people's interactions, behaviour and preferences; they are by design surveillance machines, and (ii) that different perspectives can be taken when observing people's interactions with digital media; from above (*sur*veillance), from below (*sous*-veillance), or by peers (*co*veillance).

In this commentary, I will advance the idea that as we think about and research the ethical implications of digital media by focusing on their inherent surveillance capacities, we need to be conscious about the conceptual perspective we take. While the title of this panel suggests that *perspective* is important – whether we are looking from above as a Big Brother or from below or as peers, as Little Sisters – I suggest that *perspective* is just one among a number of important conceptual constructions that needs consideration. To help guide this dialogue I will present three models of privacy that can advance thinking and research about digital media's implications for privacy protection.

Privacy has historically been conceptualised as freedom from intrusion, protection of the private sphere, the right to be left alone, and other similar notions (Solove 2008). Agre (1994) argued that the typical model for privacy has been the "surveillance model" (Agre 1994: 105), which has focused on data collection and the use of that data. I will in this commentary propose that a different model of privacy is needed when it comes to big data and digital media, namely a datafication model of informational privacy.

Informational privacy

There are currently two major conceptualisations of the privacy of (personal) information: one that regards privacy as the ability to "limit or restrict others from information about" oneself (Tavani 2008: 141) and another that views privacy as the "control of personal information" (Solove 2008: 24). Both concepts operate on the assumption that information is something that can be controlled or to which access can be restricted. Data or information are typically regarded as objective entities that exist and it is assumed, though often unarticulated, that there is a direct and true correspondence between

Mai, Jens-Erik (2016). Three Models of Privacy. New Perspectives on Informational Privacy. *Nordicom Review*, 37(special issue): 171-175. doi:10.1515/nor-2016-0031

the data or information and the actual state of affairs in the world – hence the notion of *footprints*. Footprints presume that there is a neutral and direct one-to-one relation between the traces left behind by human activity, the footprint and the actual state of that human activity. The basic premise is that people enjoy privacy when they have the abilities to control and/or restrict access to data or information about themselves – that is, when they control and/or restrict access to the footprints they leave behind (Mai 2016b).

In the age of big data, personal information has become a commodity that is traded on the market of information empires and between data brokers. Personal information is something that holds monetary value: "personal information can be viewed as a kind of property that a person can own and negotiate within the economic or commercial sphere" (Tavani, 2008: 134). The digital information society has brought about an information utopia where the use of computers and network technologies track all the activities humans engage in, though Winner (1986) suggested as early as the the mid-1980s that "as a badge of civic pride a citizen may announce, 'I'm not involved in anything a computer would find the least bit interesting'" (Winner 1986: 115).

Personal information, however, is not only valuable as singular pieces of data. Information about my age, marital status, profession, income, mortgage, address, credit score, health record, hobbies, employer etc. has some value in particular situations, but those data are only really valuable when they are assembled into a big dataset where predictive analytics is possible. In other words, when I control or restrict access to information about my recent purchases at the local petrol station I may enjoy privacy at that moment. I may decide to pay in cash, to decline their offer of a discount card, shield my face and licence plate from the CCTV cameras, etc. to protect my privacy and personal information. However, at that moment it may seem to be a relatively small piece of personal information to provide the petrol station with information about my purchases at that particular petrol station, for which the petrol station in return offers a decent discount on the already very expensive fuel. I may therefore decide to give away that small and insignificant piece of personal information to the petrol station. I get a discount and they get to know my fuel purchase pattern. Who cares how many litres of petrol I purchase anyway? However, once that information enters the pile of big data about me and my consumer segment, it is possible to gain insights about me that I may never have provided to anyone. The really interesting part is not what I purchased at the petrol station, but how that information together with other individual pieces of personal information that I have sold on the information market can reveal new information and insights about me. While I may control or restrict access to information about my fuel purchases, how would I control the new information and insights that can be computed about me from the pile of big data?

The traditional approach to restricting, limiting and controlling access to personal information "has remained largely unchanged since the 1970s" (Solove 2013: 1880). The traditional approach has been to ask people to consent to the collection and use of their personal information and the basic assumption has been that people are able to "make conscious, rational and autonomous choices about the processing of their personal data" (Schermer, Custers & van der Hof 2014: 171). This approach obviously fails today, now people are asked to enter several consent agreements on a daily basis as they navigate the digital information environment and use digital media. In some instances, people consent without reading the agreements in full, and often they do not understand the

details of the agreements they enter. In other words, the traditional approach to privacy needs to be reconceptualised and reconsidered.

The important question, however, is not whether big data and digital media increase the risk to privacy, because the right to privacy is clearly at risk in the digital information society. The real question is whether big data and digital media fundamentally change the character of the risk. If the risk to privacy is merely larger in the digital information society, then the laws and rules that currently protect privacy may still work in the new information age; all we need to do is to redouble our existing efforts. However, there are clear indications that the problem has changed. The traditional approach to privacy protection through consent and the ability to restrict, limit and control personal information comes short given new information and communication technologies. In other words, we need new solutions and new conceptual approaches to understand privacy in the digital information society.

Three models of privacy

While there have been a number of proposals for new and improved understandings and definitions of informational privacy in the digital information society, it is my sense that we need to change the metaphors we use to discuss privacy. I will here follow Agre's (1994) programmatic paper, in which he argues that the notion of privacy ought to be re-conceptualised from a "surveillance model" (Agre 1994: 101) to a "capture model" (Agre 1994: 101). I build on Agre's work and extend it with a "datafication model" of privacy – I have discussed these models in more depth in a recent paper (Mai 2016a).

The objective behind the shift in focus from *definitions* of privacy to *models* of privacy is to shift focus from establishing characteristics of privacy with the purpose of determining the definition that captures all aspects of privacy, regardless of time and place, to focus on how privacy works and how thinking about privacy shapes the language we use to discuss privacy. The purpose is not to provide a new and improved definition of informational privacy, but to suggest that in the digital information society we need to think differently about privacy – and I want to show that there is a need for a datafication model of privacy for that purpose.

I will use Agre's (1994) original, rather loose definition of a *model*, which is simply: "A 'model,' for present purposes, is a way of looking at things; specifically, it is a set of metaphors. Distinct models do not divide the world's sociotechnical phenomena into nonoverlapping classes." (Agre 1994: 105). Different models may look at the same phenomena in the world, but they will focus on different aspects and highlight different characteristics. The language used to discuss the phenomena will differ, and different models will use different metaphors to describe the phenomena. Agre operates with metaphorical components that together outline the two models of privacy. Unlike definitions, the aim is not to describe or prescribe the characteristics of privacy, but to provide metaphors that indicate how privacy functions. These following three models of privacy can help us think through the problem space and help us devise possible solutions:

The panopticon model: the metaphor of watching. This is the traditional understanding of privacy and surveillance, and also the model embedded in the language and conceptualisation of this panel. This model applies visual metaphors such as Orwell's "Big Brother is watching you" and Bentham's panopticon. The basic idea is that surveillance

and the breach of privacy is conducted by someone "watching" someone else, and it is assumed that the watching is "nondisruptive and surreptitious" (Agre 1994: 105). The model applies metaphors such as "the 'invasion' of a 'private' personal space", focuses on the "opposition between 'coercion' and 'consent'", and employs the notion of a bureaucracy's centralized orchestration of sets of 'files' and is as such often identified with "the state, and in particular with consciously planned-out malevolent aims of a specifically political nature" (Agre 1994: 106).

The focus of the panopticon model of privacy is therefore on the tensions between the watchers and the watched, between public and private spheres, and on inherent power relations.

The capture model: the notion of a grammar of action. The capture model changes focus to be primarily concerned with how human activities are constructed in "a computer system's representation languages", and as such, the model applies structural metaphors and describes the captured activity as assembled from a "'catalog' of parts provided as part of its institutional setting" (Agre 1994: 107). The organization of activities is decentralised and heterogeneous and the activities take place "within particular, local practices that involve people in the workings of larger social formations", and unlike the panopticon model, the capture model is "not political but philosophical" and the captured activity is "reconstructed through assimilation to a transcendent ('virtual') order of mathematical formalism" (ibid.).

In the capture model of privacy the focus is on the codification of activities, the sociotechnical nature of computer technology, and the unclear purposes of data collection.

The datafication model: the metaphor of patterns of behaviour. While both the panopticon and the capture model of privacy have focus on the collection of data, the datafication model of privacy has its focus on processing and analysis of data, and as such on the production of new personal information. Data collection is ontologically oriented, it focuses on data as representing facts about the state of affairs in the world: people and activities and the interrelation between places, times, other people, activities and intentions. The datafication model changes the focus to the data processing and analyses and as such is epistemological oriented; it focuses on the facts or realities that data can generate once it is processed and analysed.

In the datafication model of privacy the focus is on the anonymous creation of new personal information, the reinterpretation and statistical analysis of data, and the commodified nature of personal information.

Conclusion

The three models of privacy presented here are not competing views or approaches to informational privacy; they present three different views of the same problem sphere. The three models highlight different aspects and different perspectives of the privacy situation, and as such allow us to research and focus on different aspects of the consequences of big data and digital media in the contemporary digital information society.

The purposes of introducing these three models of privacy to this panel on Big Brother and Little Sisters are (i) to allow us to question the presumptions and understandings about privacy and surveillance that are inherent in notions such as Big Brother and Little Sisters, and (ii) to present a conceptual framework of privacy that allows

us to handle privacy challenges created by the production of new knowledge that big data analysis and digital media usages generates. These three models of privacy – and perhaps especially the datafication model of privacy – could form the ethical basis for new digital media research and practice.

References

Agre, Philip E. (1994). Surveillance and Capture: Two Models of Privacy. *The Information Society,* 10(2): 101-127.

Mai, Jens-Erik. (2016a). Big Data Privacy: The Datafication of Personal Information. *The Information Society,* 32(3): 192-199.

Mai, Jens-Erik. (2016b). Personal Information as Communicative Acts. *Ethics and Information Technology,* 18 (1): 51-57.

Schermer, Bart Willem; Custers, Bart, & van der Hof, Simone. (2014). The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology,* 16(2): 171-182.

Solove, Daniel J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review,* 126: 1880-1903.

Solove, Daniel J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Tavani, Herman T. (2008). Informational Privacy: Concepts, Theories, and Controversies, pp. 131-164 in Himma, Kenneth E. & Tavani, Herman T. (eds.) *The Handbook of Information and Computer Ethics*. Hoboken, NJ: Wiley.

Winner, Langdon. (1986). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press.