Introduction to the Special Issue on the Ethics of State Mass Surveillance

Peter Königs

This is the post-print version. For the published version, go to https://www.degruyter.com/view/journals/mopp/ahead-of-print/article-10.1515-mopp-2020-0008/article-10.1515-mopp-2020-0008.xml

Recent decades have seen an unprecedented proliferation of surveillance programs by government agencies. This development has been driven both by technological progress, which has made large scale surveillance operations relatively cheap and easy, and by the threat of terrorism, organized crime and pandemics, which supplies a ready justification for surveillance. For a long time, mass surveillance programs have been associated with autocratic regimes, most notoriously with the German Democratic Republic and the *Stasi*, its secret police. A more recent case in point is the efforts of the People's Republic of China to set up a comprehensive surveillance system that assigns citizens a score reflecting their social and political conformity (Denyer 2018).

But the current rise of state mass surveillance is mostly attributable to the new readiness of liberal democracies to monitor their populations. The vast surveillance system uncovered by whistleblower Edward Snowden is maintained and supported by a group of established liberal democracies, including the United States, the United Kingdom, Canada, and many others. While surveillance programs of authoritarian regimes, installed to monitor and quash political dissidents, are uncontroversially unjust, surveillance operations carried out by liberal democracies possess at least some prima facie legitimacy. They are set up with the stated objective of protecting citizens against terrorism, organized crime and pandemics, which few would deny is the duty of any state. Still, the expansion of large-scale surveillance by democratic governments has widely been perceived as objectionable or at least problematic on account of its harmful effects on both individuals and liberal society at large.

Philosophers, however, are only beginning to study the social and political significance of state mass surveillance. As Kevin Macnish observes, 'it is curious that a practice as controversial and central to human life as surveillance has received so little sustained ethical reflection.' (2018a, p. 1) Much of the still nascent philosophical debate about the rights and wrongs of surveillance has revolved around the concept of privacy. In order to understand the harm caused by state mass surveillance, we need, it seems, an account of the value of privacy and of how privacy is affected by surveillance. And whereas surveillance itself is very much an under-researched topic in philosophy, there is a rich body of research on privacy.

One important issue concerns the concept of privacy itself. Privacy scholars have long been divided about whether privacy ought to be understood in terms of control over one's personal information or in terms of non-access to it. This controversy has a direct

bearing on how we should conceive of the impact of state mass surveillance on people's privacy. The control account, championed for instance by Charles Fried (1970), Adam Moore (2003) and Beate Roessler (2005), holds, roughly, that people's privacy is reduced as soon as they lose control over who accesses their personal information, irrespective of whether the information is accessed or not. By contrast, according to the access account, which is associated, for instance, with Anita Allen (1988), Ruth Gavinson (1980) and Macnish (2018b), a person's privacy is only reduced when her personal information is actually accessed. This definitional question matters for the evaluation of surveillance in that many contemporary surveillance operations by governments involve the massive collection of personal information but little actual access to them by a human person. In this respect, contemporary surveillance efforts differ markedly from 'old school' surveillance operations, as carried out for instance by the *Stasi*, which typically involved a human agent prying into someone's private affairs. Now, if, as Macnish suggests, the access account should be preferred over the control account, this would have the startling implication that, strictly speaking, contemporary surveillance efforts leave citizens' privacy intact. While they arguably entail a loss of control over people's personal information, they rarely involve access. This would mean, perhaps astonishingly, that they do not reduce people's privacy (Macnish 2018b, see also Ryberg 2007).

The dominant view, however, is that state mass surveillance is problematic on the grounds that it constitutes a massive violation of citizens' privacy. Privacy is, in the first instance, a good that benefits individuals, for instance as a precondition of personal autonomy. State mass surveillance thus causes harm on the individual level (Roessler 2005, pp. 119-129). But by many, privacy is also seen as a social good, as essential for democratic self-governance and as a prerequisite of political freedom (Roessler and Mokrosinska 2013, 2015). One source of concern is that state mass surveillance may have a dampening effect on democratic deliberation. There are fears that surveillance produces 'chilling effects', discouraging citizens from expressing their political opinions and engaging in other legitimate political activities (Lyon 2018, pp. 65-69; Solove 2006). These fears have been supported by empirical studies (Penney 2016, 2017). State mass surveillance threatens to damage the public sphere, the integrity of which is widely regarded as essential to democratic functioning (Stahl 2016). Another source of concern is the precarious power imbalance between the state and its citizens that extensive surveillance infrastructures are bound to generate and which, on some accounts, undermines the freedom of a society (Hoye and Monaghan 2018; Roberts 2014).

At the same time, surveillance can serve legitimate purposes, and all surveillance operations are not equally problematic. One important task for philosophers is therefore to formulate standards that allow us to determine when and which forms of surveillance may be permissible or, indeed, desirable (Henschke 2017; Macnish 2014; Moore 2011; I. Taylor 2017).

Indeed, although the rise of mass surveillance in democratic societies is mostly viewed with considerable concern, a minority of philosophers have been quite positive about surveillance. One rare enthusiast about state mass surveillance is James Stacey Taylor, who has recommended expanding the surveillance state until all citizens are monitored 'at all times and in all places.' (2005, p. 227) His argument to this effect is

an extrapolation of the uncontroversial assumption that law enforcement agencies have the right to gather information about past events, for instance by requiring witnesses to testify in court. A similarly contrarian case for state mass surveillance has been made by Ingmar Persson and Julian Savulescu. Their endorsement of surveillance is motivated by the fear of a catastrophic terrorist attack with biological or nuclear material, which could wipe out millions of lives. With the stakes so high, they suggest that liberal democracies become less liberal and expand their surveillance infrastructures, claiming also that the existence of a moral right to privacy is questionable (2012). Finally, the case that NSA's highly controversial surveillance operations are justifiable has, somewhat remarkably, been made by notable libertarians, a group that is not known for approving of the expansion of the state's power apparatus (Pilon and Epstein 2013).

This special issue features six articles that advance our understanding of the ethics of state mass surveillance. Jointly, they provide a comprehensive and balanced picture of the ethical and political significance of state mass surveillance, highlighting both the dangers associated with surveillance as well as its potential legitimate uses.

The first two contributors, Kevin Macnish and Leonhard Menges, both locate their discussions of state mass surveillance within the context of the long-standing controversy between control theorists and access theorists.

As mentioned above, Macnish previously argued that privacy is diminished only if personal information is accessed. This already suggested that state mass surveillance rarely involves diminutions of privacy. A still unexplored question, however, was if a privacy diminution occurs if private information is accessed and processed by an automated system rather than a human person. In his contribution, Macnish defends the view that contemporary state mass surveillance systems, which rely on computers to collect and process private data, do not entail a loss of privacy. Although computers may be said to access these data, he maintains that access to personal information is a necessary but not a sufficient condition for a privacy loss to occur. In addition, it must be the case that the entity that accesses the data possesses a semantic understanding of the information accessed. Since an automated system lacks this capacity, its accessing and processing people's data entails no diminution of privacy. This finding carries over to the automated collection and processing of data by private companies such as Google or Amazon. While this means that the preoccupation of both surveillance scholars and regulators with privacy issues has been misguided, Macnish is adamant that it does not mean that mass surveillance is unproblematic. Indeed, one problem is the loss of control over one's information, even though to characterize it as involving a loss of privacy would be confused.

Menges offers a subtle defense of the control account of privacy. His case for the control account revolves around so-called threatened loss cases, which provide the principal counterargument that control theorists must defuse. In threatened loss cases, a person's information is readily available to others but is not actually accessed. Think of a person who leaves her diary on a table in a coffee shop, thereby making it possible for others to read it, but who returns to the coffee shop to collect her diary before it is read by anyone. As she seems to have temporarily lost control over her personal information but as it is also implausible to assume that her privacy was diminished,

threatened loss cases seem to support the access account over the control account. Menges, however, presents a strategy that allows control theorists to both capture the intuition that privacy is not diminished in threatened loss cases and to hold on to the view that control, not non-access, is essential for privacy. Drawing inspiration from Frankfurt cases, Menges suggests that a person has control over her personal information if she is the right kind of source of the flow of information, if information flows at all. Since in threatened loss cases, no information flow takes place, privacy remains intact. This has again direct implications for how we ought to think about state mass surveillance operations, which can be described as massive threatened loss cases. Menges, although adopting a version of the control account of privacy, therefore concurs with Macnish that such operations should not be said do constitute privacy invasions. He also, however, concurs that surveillance may be objectionable nonetheless, if primarily for privacy-unrelated reasons.

The contributions by Patrick Taylor Smith and Titus Stahl analyze the political significance of state mass surveillance, especially its impact on the freedom and the democratic functioning of a society.

Smith provides a neo-republican theory of just state surveillance. He observes that extensive state surveillance is both a necessary means of enhancing freedom in the neo-republican sense as well as a possible threat to this freedom. It enhances freedom, and is therefore legitimate, to the extent that it is used to protect people from private domination, such as organized crime. At the same time, it poses a threat to freedom in that it entails the risk of public domination by augmenting the power apparatus of the state. Critical of technological solutions to the threat of public domination, Smith presents an institutional strategy of containing the power of the surveilling state and at the same time allowing it to perform its duty of preventing private domination. The key role in this institutional solution is played by technology companies. Smith suggests that tech companies be institutionally incentivized and empowered to protect their users' privacy against unjust privacy violations by state agencies. His suggestion has two components: First, he suggests extending the civil liability of tech companies for the misuse of their users' data. This will provide tech companies with a strong financial incentive to pressure the government to deal responsibly with the data that tech companies provide them with. Second, he proposes that civil society actors 'occupy' tech companies, that is, that they be represented within their decision-making bodies, so as to be able protect users' privacy interests in a more direct fashion.

The focus of Stahl's contribution is on how state mass surveillance impacts the democratic public sphere and the functioning of democratic decision-making. Taking issue with the notion that privacy should be reserved for activities that one seeks to conceal from the public, he contends that political activities, which are intentionally public in that their very purpose is to address the public, deserve privacy protections, too. His argument for this claim is inspired by Jürgen Habermas' theory of deliberative democracy. According to Habermas, the political deliberation that takes place within the public sphere plays the crucial role in the generation of political legitimacy. Stahl maintains that surveillance undermines the legitimacy of political decisions by affecting the way in which people participate in democratic deliberation, thereby compromising the functioning of the public sphere. Specifically, the problem with surveillance is that it may induce the participants in the public sphere to engage in strategic action rather

than in the sort of purely communicative action that is required for the generation of political legitimacy. Surveillance then also erodes the trust of the audience in the speaker's communicative sincerity. The result is that surveillance undermines the capacity of the public sphere to function as the producer of legitimate political decisions.

Finally, the contributions of Frej Thomsen and Adam Henschke investigate the ethics of specific surveillance practices: police body-worn cameras and the Internet of Things.

Thomsen makes a cautious case for the use of police body-worn cameras (PBWC). After reviewing the empirical evidence on the effects of PBWCs, he presents a teleological argument in defense of their use. One key premise of this argument is that the good that PBWCs bring about outweighs the bad. The benefits of PBWCs include deterrence of police misconduct and of unwarranted complaints against police officers, whereas the problem of chilling effects and the potential misuse of the data for blackmail, humiliation or retaliation are some of the major drawbacks. Since the good is assumed to outweigh the bad, his teleological argument concludes that the police ought to use PBWCs, unless there are compelling deontological considerations that override or outweigh the teleological reason for using them. Thomsen therefore proceeds to discuss possible deontological objections. He reviews two arguments that might provide such a deontological reason against PBWCs. One possible deontological objection is that the use of PBWCs is mistrustful in a morally problematic way. A second possible deontological objection is that the use of PBWCs constitute a violation of people's privacy rights. Thomsen finds neither worry to be compelling, concluding that, in the light of the teleological reason, we should welcome and encourage the use of PBWCs, at least under certain favorable conditions.

Henschke's contribution focuses on conceptual and ethical issues related to the Internet of Things, which can be a formidable tool for state surveillance. In contrast to Macnish and Menges, Henschke advocates taking a pluralist approach to privacy, allowing that privacy can have different meanings in different contexts. Whether the Internet of Things and its use for state surveillance purposes should be characterized as jeopardizing people's privacy depends on whether we adopt the interpersonal or the political conception of privacy. The interpersonal conception casts privacy as a relation between people interacting with each other, whereas the political conception casts it as a relation between citizens and the state. Interpersonal privacy is primarily about what Henschke calls thick personal information, that is, about personal information that is meaningful to people as semantic agents. Political privacy, by contrast, is primarily about the power relations between the state and the citizens whose information are gathered and processed. Considered through the lens of the interpersonal conception of privacy, the Internet of Things, being a non-human, non-semantic system, is relatively innocuous, although it does involve some potential for interpersonal privacy violations. If we adopt the political conception, however, the Internet of Things when used as a tool for state surveillance is highly problematic, entailing genuine privacy violations.

The current rise of mass surveillance practices by democratic governments raises pressing ethical, political and conceptual questions, which the contributions to this special issue go a long way towards answering. But more than that, they also offer

valuable insights into related issues, such as the concept and value of privacy, the significance of surveillance by non-state actors, as well as into the nature of free and democratic society.

References

Allen, A. (1988). *Uneasy Access. Privacy for Women in a Free Society* (Totowa, NJ: Rowman and Littlefield).

Denyer, S. (2018). 'China's Watchful Eye', *The Washington Post*, URL = https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/, 7th January.

Fried, C. (1970). *An Anatomy of Values* (Cambridge, MA: Harvard University Press).

Gavinson, R. (1980). 'Privacy and the Limits of Law', *Yale Law Journal* 89 (3): 421-472.

Henschke, A. (2017). *Ethics in an Age of Surveillance. Personal Information and Virtual Identities* (Cambridge: Cambridge University Press).

Hoye, J. M. and Monaghan, J. (2018). 'Surveillance, freedom and the republic', *European Journal of Political Theory* 17 (3): 343-363.

Lyon, D. (2018). *The Culture of Surveillance* (Cambridge: Polity Press).

Macnish, K. (2014). 'Just Surveillance? Towards a Normative Theory of Surveillance', *Surveillance and Society* 12 (1): 142-153.

Macnish, K. (2018a). *The Ethics of Surveillance. An Introduction* (Abingdon: Routledge).

Macnish, K. (2018b). 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World', *Journal of Applied Philosophy* 35 (2): 417-432.

Moore, A. (2003). 'Privacy. Its Meaning and Value', *American Philosophical Quarterly* 40 (3): 215-227.

Moore, A. (2011). 'Privacy, Security, and Government Surveillance. Wikileaks and the New Accountability', *Public Affairs Quarterly* 25 (2): 141-156.

Penney, J. W. (2016). 'Chilling Effects. Online Surveillance and Wikipedia Use', *Berkeley Technology Law Journal* 31 (1): 117-182.

Penney, J. W. (2017). 'Internet Surveillance, Regulation, and Chilling Effects. A Comparative Case Study', *Internet Policy Review* 6 (2): 1-39.

Persson, I. and Savulescu, J. (2012). *Unfit for the Future* (Oxford: Oxford University Press).

Pilon, R. and Epstein, R. A. (2013). 'NSA Surveillance in Perspective', *Chicago Tribune*, 12th June.

Roberts, A. (2014). 'A republican account of the value of privacy', *European Journal of Political Theory* 14 (3)*:* 320-344.

Roessler, B. (2005). *The Value of Privacy* (Cambridge, MA Polity Press).

Roessler, B. and Mokrosinska, D. (2013). 'Privacy and Social Interaction', *Philosophy and Social Criticism* 39 (8): 771-791.

Roessler, B. and Mokrosinska, D. (eds.)(2015). *Social Dimensions of Privacy. Interdisciplinary Dimensions* (Cambridge: Cambridge University Press).

Ryberg, J. (2007). 'Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs Aremac', *Res Publica* 13 (2): 127-143.

Solove, D. (2006). 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* 154 (3): 477-564.

Stahl, T. (2016). 'Indiscriminate mass surveillance and the public sphere', *Ethics and Information Technology* 18 (1): 33-39.

Taylor, I. (2017). ‘Data collection, counterterrorism and the right to privacy’, *Politics, Philosophy & Economics* 16 (3): 326-346.
Taylor, J. S. (2005). ‘In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance’, *Public Affairs Quarterly* 19 (3): 227-246.