



Kevin Macnish: The ethics of surveillance: an introduction

Routledge, London and New York, 2018, ISBN 978-1138643796, \$45.95 (Pb)

Tony Doyle¹

© Springer Nature B.V. 2019

Kevin Macnish has made significant contributions to the surveillance and privacy literature during the past decade. So I welcomed the publication of *The Ethics of Surveillance*, a clearheaded, agenda-free, chock-a-block-with-case-studies text. In addition to serving as a fine introduction to the field, Macnish's book offers a lot for scholars who follow the debate on surveillance and privacy. Macnish is also clear about his orientation: He's an analytic philosopher whose sympathies are firmly liberal democratic. He takes a broadly consequentialist approach, while emphatically rejecting act utilitarianism.

Macnish assumes that, although surveillance is often morally justified, the burden should be on the surveillant. All morally permissible surveillance has to be prompted by a just cause. Once this condition is met, the practice will ideally meet the following conditions in which it should:

1. be necessary to detect the harmful or undesirable activity in question.
2. be proportionate to that activity's moral gravity. (So tapping the phone of a serial killer would be justified, assuming that the snooping was necessary to track him down. The loss of privacy of the innocent people with whom he is chatting is worth it given the gravity of his crimes. Not so a serial shoplifter: Even if there were no "alternative means" of catching him, the procedure would be disproportionate to the offence. After all, the data and metadata of many who are not culprits—or "morally liable" for surveillance, to use Macnish's phrase—will be scooped up too.)
3. occur with the consent of the surveilled.
4. be conducted by an accountable authority.

✉ Tony Doyle
tdoyle@hunter.cuny.edu

¹ Hunter College Philosophy Department, Hunter College Library, 695 Park Avenue, New York, NY 10065, USA

However, Macnish is quick to acknowledge that there will be cases of permissible or even obligatory surveillance where either the third or fourth condition is not met. For example, we would not expect the police to get the consent of a suspected serial killer before putting him under 24-7 surveillance! Nor need all permissible surveillance be conducted by an accountable authority, as when a bystander records a bank robbery or police abuse on her phone.

The Ethics of Surveillance is divided into two parts. The first covers general issues in the ethics of surveillance: when it is justified, why it is sometimes problematic, the relationship between privacy and surveillance, and the non-privacy harms of surveillance. Part One also provides a useful survey of the recent literature, which Macnish knows well. Part Two deals with specific issues in surveillance, like national security, surveillance of public places, commercial uses of big data analytics, and workplace surveillance. I will discuss each below.

Macnish offers a broad working definition of *surveillance*, while also not insisting on necessary and sufficient conditions for the correct application of the concept. After all, undergraduates do not need a counterexample-proof analysis. He suggests that surveillance has to go beyond "a casual glance, or overheard snippet of conversation" (p. 10). Instead, it involves "sustained monitoring of a person or people" that covers everything from watching or listening to pure data collection or "dataveillance," where the surveillants never see or hear us (pp. 10, 11).

The text also devotes considerable space to the ethics of privacy, since in Macnish's view violations of privacy are "probably the most obvious wrong to arise from surveillance" (p. 31). Plausibly passing on a definition, he suggests that privacy's value lies chiefly in increased autonomy and reduced harm. In short, privacy tends to promote the good life. Today's leading challenge to privacy comes from ubiquitous surveillance and big data analytics, both of which have radically transformed the flow of information. Those

analytics have time and again yielded surprising and often sensitive inferences about us from far-flung, innocuous, and seemingly unrelated pieces of data. The cost to privacy is incalculable. Privacy skeptics and staunch surveillance advocates have pushed back, however, arguing that those who have nothing to hide have nothing to fear from today's regime of massive collection, rigorous analysis, and broad distribution of personal information. This view has been most prominently defended by Richard Posner, who sees most appeals to privacy as self-serving or even fraudulent attempts to gain an advantage over others (Posner 1978). Not true, says Macnish. He focuses specifically on state surveillance. If the skeptic's argument is sound, he says, "then it amounts to a justification for blanket surveillance by the state" (p. 67). To oppose state surveillance "is tantamount to confessing guilt" (p. 67). Moreover, the nothing-to-hide doctrine places undue confidence in the "benevolence" of even enlightened, liberal democratic states (p. 67). Also, minorities generally have more to fear from an information-empowered state than non-minorities. Whistleblowers too, Macnish observes, have much to lose from no-holds-barred surveillance, since "they would be exposed the moment they raised an issue" (p. 67). Macnish's point is well taken.

As stated above, the second part of the book is dedicated to specific issues in the ethics of surveillance. I will focus here on national security and counter-terrorism, the surveillance of public places, the commercial uses of surveillance, and workplace surveillance.

One popular argument for the massive and indiscriminate surveillance of citizens is that terrorism represents a grave, even existential, threat to liberal democracy and can be reliably detected only if everyone is surveilled. Of course, this means that most of those affected will not be morally liable for surveillance; the practice involves treating everyone as a potential terrorist. Defenders of this approach point to advances in data scientists' ability to detect the anomalous patterns characteristic of terrorists' exchanges. In short, if you are looking for a needle, add hay. Macnish thinks that we should resist this approach, since it has potentially staggering social costs. As he persuasively puts it,

The goal of any such system is to reach a state of no false positives and no false negatives, so that everyone identified by the system is someone who is of interest, and that no one who is of interest goes unidentified. However, it is questionable whether this is ever achievable, especially when those who are deemed of interest fall into vague categories such as 'terrorist' or 'criminal'.... The result is that there are people who are incorrectly identified as threats, and then harassed and stigmatized as a result. (p. 39)

Another reason for resisting comprehensive government surveillance is that any liberal democracy worth its salt should

be fully accountable to its citizens. Macnish implies that it cannot be if its citizens do not know that they are subject to indiscriminate snooping. Also, he points out that most terrorist plots are hatched in people's homes, and not even the stoutest defenders of surveillance have had the cheek to call for blanket surveillance there.

Commercial surveillance must surely rival government surveillance as a threat to privacy. In fact, commercial entities are likely to have far more information about us collectively than the government does, given our phones, credit cards, browsing behavior, online shopping, streaming subscriptions, and social media accounts. For the most part, in the United States at least, commercial surveillance proceeds with scant accountability. An important motivation for commercial surveillance is to capture attention for targeted ads. Macnish gets it: Businesses naturally want maximum bang for the advertising buck. Ideally, all and only actual or potential customers would see a given company's ads: No false negatives, no false positives. Big data analytics promises to converge on this ideal in a way inconceivable in the old days of "small" data. Surveillance becomes profiling: The more data gathered and the more sophisticated the analysis, the more accurate the resulting portraits.

Colossal collection, combined with wily analytics, permits ever-finer social sorting, which in turn can prod people's vulnerabilities. Those who are slotted as poor are more likely to see ads for, say, predatory loans or for-profit "universities" which exploit their poverty. On the other hand, they will be denied many of the discounts offered to the wealthy and well-to-do. Big data profiling, then, can exacerbate inequality. Deliverance was supposed to come from notice and choice. The regime looked promising at first: Inform us of all the ways in which our information might be used, and let us decide, in the light of this, whether to opt in. However, to cover all contingencies, the statements soon grew criminally technical and monumentally long, calculated to gravel even a professor of contract law. As a result, approximately no one reads them. Refusal to accept the terms means denial of service. Macnish offers an apposite medical analogy: "Would we be happy with a doctor performing surgery on a fully competent adult, knowing that the adult had only skimmed through the consent document before signing it?" (p. 149). For good measure we might throw in that the thing sprawls to 20,000 words, is unfathomable, and can be changed between the time that the patient has signed it and the moment she goes under the knife.

Another response to the depredations of commercial big data is "propertization," which calls for assigning property rights to data subjects in the information that companies glean about them. Macnish is skeptical. First, where should we draw the line about what counts as "my" information? The length of my hair? The fact that I breathe oxygen? Or suppose, at the other extreme, we say that personal data is

only that information which I am able to keep private. “If so, as soon as [someone else] accesses the data, it ceases to be personal” and thus would be up for grabs (p. 149). Second, the trouble is we do not think of our own information in the same way that we think of either physical property or standard intellectual property. Both types are alienable: Once I’ve sold you my 2011 Civic or the movie rights to my latest pot boiler, you are legally free to dispose of them as you see fit. However, Macnish rightly suggests that most people would balk at having their information shuffled around like this. If I sell you the list of all the music that I’ve listened to over the past 3 months or key details about my last five vacations, I might want to have a say about who you hand it off to: large datamongers, marketers, insurers, banks, landlords, law enforcement, or potential employers. And even if I do not own data that relates to me, it does not follow that others should be able to have their way with it. To use Macnish’s example, I might not own my medical records, but it does not follow that my doctor would be justified in making those files available to my boss or insurer without my permission. Propertization is a dead end.

Regarding workplace surveillance, Macnish emphasizes how digitization and networking permit far closer monitoring than ever before. Generally, the higher one’s socioeconomic status, the less workplace surveillance one will be subject to. Those working in fast food or retail might have cameras fixed on them at all times. Call center responders could have their every exchange monitored. Hourly employees generally punch a time clock. However, even those with high status jobs use company computers, where every keystroke is recorded. Many also have company phones, which can trace their steps round the clock. Macnish is understandably worried that the new surveillance regime is blurring “the more traditional home/work divide” (p. 175). Although solid, this chapter might have said something about the asymmetries between employer and employee. After all, employers are not just any surveillants. First, there is an information asymmetry: The man knows much more about us than we know about him. Second, a related power asymmetry means that employers control the conditions of employment and can decide who is passed over for promotion or who gets fired. Employees often have little recourse.

As for surveillance of public spaces, Macnish affirms a “reasonable” expectation of privacy in public. For instance, it is reasonable for me to expect that, while in a restaurant, “the restaurateur has [not] placed a microphone in the flowers on the table and is listening to [my] every word” (p. 34). Even though many can see me as I walk down Main Street at high noon, I am justified in believing that my image will not join a vast sharable file of other images of me. Macnish is also concerned about the extent to which public surveillance can chill protests or discourage unconventional, but morally permissible, behavior. Moreover, as we have seen, Macnish

contends that, other things being equal, surveillance should be targeted, as against blanket, and should focus on those who are morally liable for it rather than not. Although he is not unconditionally opposed to the practice, public surveillance obviously gets low grades here. Macnish is exercised about the prospect of being monitored whenever we leave the house. We are well on the way to creating a “ring of steel through which people cannot pass unmonitored” (p. 196). Macnish suggests that this is a bad idea. He’s right.

Before concluding, I would like to hazard two criticisms. What I say here might be better thought of as suggestions for a second edition, which I hope will be down the road.

First, Macnish offers a brief but lucid account of how big data analytics can mess with privacy. He adduces Target’s much-discussed pregnancy “scores,” which derive from mostly non-sensitive information about purchasing history. The scores were an attempt to determine how likely customers were pregnant given what they had bought. However, he ignores the glut of false positives associated with the case: Probably most women who received Target’s baby-related coupons were not pregnant, which explains why the company included other offers for, say, wine glasses in the same mailing (Harford 2014). This casts doubt about whether even the pregnant women who got Target’s babywear coupons had their privacy violated.¹

Leaving aside concerns about false positives, Target’s program is a case of what Baracos and Nissenbaum (2014) call the “tyranny of the minority.” It only takes a few people to reveal certain of their traits or habits to enable third parties to make privacy-threatening inferences about the many others who have made no such disclosure but who happen to share other more manifest traits with the minority. This raises a problem for Macnish’s assumption that the distinction between consensual and non-consensual surveillance is “core” to the debate about the ethics of surveillance (p. 48). As the Target case shows—or a more refined case with fewer false positives would show—consent is increasingly beside the point in the era of big data (Baracos and Nissenbaum 2014). Once a representative sample of the shopping or browsing habits of others relevantly like me exists, data scientists can make unbidden and potentially unwelcome inferences about me and my ways.

Also, consider a criticism that Macnish offers of act utilitarianism. The view, he says, “has fallen out of favor in contemporary philosophy for a number of reasons, not least that it could lead to the justification of isolated, extreme or repellant acts so long as they led to the greatest good. The Panopticon is such an example, and is repellant to many today for the way in which the inhabitants would be subjected to constant surveillance” (p. 16). Yes, but anxiety

¹ I would like to thank Don Fallis for this suggestion.

regarding constant surveillance will undermine utility and to that extent will count against the practice for the act utilitarian. So it is not clear that the act utilitarian has to endorse the Panopticon, even if Bentham did. He also claims that Bentham's Panopticon became a model for the Soviet Union and Nazi Germany. This is unfair to Bentham, since he insists that the watchers be under precisely the same kind of scrutiny, and thus accountability, as the watched (Bentham and Božovič 1995).

Today's Panopticon, compliments of big data, is conspicuously different from Bentham's: (1) much, much more information is collected; (2) that information can be aggregated efficiently, meaning that widely dispersed information about you or me can be available from a single point; (3) data analytics permit hitherto undreamt of inferences about our traits, habits, commitments, and vulnerabilities; (4) the information can be distributed to myriad third parties in no time; (5) not only the government but also countless non-governmental data holders can use this information against us. A modern Benthamite would have deep qualms about the new Panopticon. To be fair, Macnish appreciates the problem: "With the advent of smartphones, smart televisions, and game components like Xbox Kinect, with which manufacturers can gain visual and aural access to the room in which they are placed, many people... today live in a world dominated by Orwell's telescreens. However, unlike Orwell's world, in ours these have not been imposed by the government. Rather we have, like Huxley's citizens [in *Brave New World*], invited them into our homes, seduced by the pleasures they can bring while oblivious to the risks they present" (p. 16). Right, but don't blame Bentham or his twenty-first century successors.

As mentioned at the outset, Macnish was a strong choice to write this text. He has discharged his task admirably. Too

many introductory texts in philosophy read like they are aimed at third-year graduate students. Macnish, by contrast, shows a commendable sense of his audience. A couple hiccoughs notwithstanding, his text is generally free of jargon and undue technicalities; abstract and general claims are supported with relevant and useful examples. Although he does not try to hide his own views, he never permits them to crowd out ideas he might disagree with. All reasonable positions get a fair hearing. Macnish suggests that the book is intended to prompt his readers to think "more deeply and more carefully" about the ethics of surveillance (p. 212). It will. His hope is that it will help to transform the way that policy makers and their constituents think about surveillance in the future. Mine too.²

References

- Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 44–75). New York: Cambridge University Press.
- Bentham, J., & Božovič, M. (1995). *The Panopticon writings*. London and New York: Verso.
- Harford, T. (2014). Big mistake. *Significance*, 11(5), 14–19.
- Posner, R. (1978). An economic theory of privacy. *Regulation*, 2, 19–26.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

² I would like to thank Jane Carter and Don Fallis for their comments.