CHAPTER 1

SURVEILLANCE ETHICS: AN INTRODUCTION TO AN INTRODUCTION

Kevin Macnish

ABSTRACT

This short chapter is an introduction to my 2018 book: The Ethics of Surveillance: An Introduction *(Macnish, 2018). It is provided at the start of this PRO-RES collection of essays because it anticipates and supplements the range of issues covered in this collection and lays out some of the fundamental considerations necessary to ensure if surveillance must be conducted, it will be done as ethically as possible.*

When is surveillance justified? We can largely agree that there are cases in which surveillance seems, at least prima facie*, to be morally correct: police tracking a suspected mass murderer, domestic state security tracking a spy network, or a spouse uncovering partner's infidelity. At the same time, there are other cases in which surveillance seems clearly not to be justified: the mass surveillance practices of the East German Stasi, an employer watching over an employee to ensure that they do not spend too long in the toilet, or a voyeur watching the subject of his lust undress night after night.*

As an introductory text, my book does not seek to provide a list of necessary and sufficient conditions for ethical surveillance. What it does provide is an overview of the current thinking in surveillance ethics, looking at a range of proposed arguments about these questions, and how those arguments might

Ethical Issues in Covert, Security and Surveillance Research
Advances in Research Ethics and Integrity, Volume 8, 9–16

ISSN: 2398-6018/doi:10.1108/S2398-601820210000008002

play out in a variety of applied settings. It hence provides a useful and accessible volume for policymakers wishing to rapidly get up to speed on developments in surveillance and the accompanying ethical discussions.

Keywords: Surveillance; ethics; privacy; espionage; security; public sector

INTRODUCTION

My book is divided into two parts. The first part provides an historical overview of ethical engagement with practices of surveillance, before turning to the more philosophical issues which serve as a foundation to discussions on surveillance ethics. The second part moves on to a survey of different applied situations in which surveillance raises persistent challenges in the twenty-first century. Each chapter includes case studies throughout and ends with a bulleted summary and questions for discussion. I shall take each in turn in this introductory summary.

SECTION ONE

The opening chapter on the history of thought on surveillance ethics begins with reflecting on how to define the term. Several definitions have been proposed, but most, such as those by David Lyon (2007) or the Surveillance Studies Network 2006 report for the UK Information Commissioner's Office (Ball, Lyon, Murakami Wood, Norris, & Raab, 2006), contain a sense of purpose within the definition (such as care, control, and entitlement). This leads to the challenge that an act which appears to be surveillance would not in fact be such if the purpose lay outside the list of purposes provided. Without denying the value of a definition, the preferred approach is to opt for a working definition which equates surveillance with monitoring but leaves it there. From here, the chapter progresses to consider discussions of surveillance in ancient, medieval, and modern times. This historical review ranges from biblical commands through the introduction of eavesdropping laws to the development of spy satellites in the Cold War. More recently still has been the radically transformative introductions of the internet and CCTV. Finally, the chapter considers contributions to ethical reflections on surveillance from both western and non-western traditions.

The second chapter turns to the wrongs of surveillance, most obviously wrongs related to privacy (which receives due attention) but also non-privacy wrongs which may be overlooked in public discourse. These include impacts on trust, chilling effects (the muting of democratically legitimate activities for fear of persecution, heightened by surveillance), power and control, bureaucratic error and false positives, and social sorting (the division of societal groups through surveillance techniques). It closes with a philosophical reflection on the implications of so-called harmless surveillance. Here it picks up on a paper by Tony Doyle (2009), imagining an alien light years from Earth and hence unable to have an impact on

our lives. This is brought into a more applied setting when considering historical research into the dead, such as exhuming the body of Richard III or breaking the cypher used by Samuel Pepys in writing his diary.

The final chapter of the first part outlines key ethical issues in surveillance. The first such issue surrounds questions of consent, noting that most ethical issues surrounding surveillance concern non-consensual surveillance. However, these are, importantly, not the only ethical issues, and the chapter looks in some depth at ethical problems which may arise from consensual surveillance, picking up on the work of Alan Wertheimer (1999, 2006) to look at questions of coercion and exploitation in apparently consensual acts of surveillance. The more substantial part of the chapter is dedicated to non-consensual surveillance, though. Here several issues are discussed, including the cause and context of the surveillance; the authority for the surveillance and attendant issues of paternalism; proportionality and necessity; and discrimination and deterrence. The final section turns to two populist arguments and thoroughly dismisses both: the suggestion that, 'if you have done nothing wrong then you should have nothing to hide', and the politician's canard that we need to make a trade-off between privacy and security, which is always raised during times of heightened insecurity. Neither of these positions turns out to be convincing on reflection.

SECTION TWO

With the foundational theoretical work in place, the book moves to the applied section. This second section looks at ethical questions pertaining to a variety of contexts, starting with state surveillance (espionage, security, policing, and social welfare), before considering corporate practices (espionage, commerce, journalism, private investigation, and workplace surveillance), and finally two broader topics: surveillance in public places and surveillance of the very old and the very young. Of the applied areas under consideration in the book, the ethics of espionage has perhaps the greatest philosophical engagement, followed by policing. Areas, such as private investigation and surveillance of the young, have received comparatively little attention to date, making many of these chapters unique as introductions.

The ethics of espionage is one area, though, which does have a long history, and one which intertwines with that of surveillance for obvious reasons. That espionage is not tantamount to surveillance can be seen through tactics such as 'turning' agents or torturing suspects, neither of which could be considered monitoring (Macnish, 2016). However, a clear overlap exists between the practices which has only grown through the twentieth century boom in signals intelligence, which is essentially a form of industrial-scale surveillance. This history provides an opportunity to reflect on different ethical approaches to the ethics of espionage, from deontological and consequentialist frameworks through to reciprocal approaches and those, including my own, which favour appeal to the just war tradition for guidance (see, e.g. Bellaby, 2014; Macnish, 2014; Omand, 2012; Quinlan, 2007). Further issues which merit discussion include the so-called

Coventry Dilemma, in which a leader must decide whether to allow a city to be obliterated to mask the fact that they are reading the enemy's communications, and the question as to whether it is acceptable to spy on allies and civilians.

The following chapter on state security picks up on the ethics of monitoring civilians, shifting the focus from the civilians in another state to those in one's own state. Where this might be justified in cases where state security has evidence that a civilian is involved in acts which are seriously detrimental to the life of the state (e.g. terrorism), the question remains as to how to find this evidence in the first place. This turns the conversation to issues of mass surveillance and the potential justification which may be sought in the doctrine of double effect. Several problems are raised with this appeal, though, and so an alternative approach in appealing to apparently less privacy-invasive data analytics is brought into the spotlight. Again there are problems here, though, including the collection of data about those known to have done nothing to merit surveillance and the general bluntness of the approach. The chapter closes with a review of ethical challenges with encryption, which rarely seems far from the headlines, and corporate involvement in state security practices.

The chapter on policing follows naturally from that on state security, and also picks up on the challenges of uncovering the evidence necessary to justify targeting surveillance on a particular individual or group. One such solution is that of undercover policing, itself a form of surveillance but one which is more targeted than mass surveillance. This, though, as has become apparent in the UK following a string of scandals, is also highly controversial as police have targeted groups of no apparent threat to the state and officers fathered children with activists before disappearing from their lives, an act seemingly condoned by their commanding officers (Nathan, 2017). The relatively recent introduction of body worn cameras is considered before a final, somewhat more philosophical debate is introduced as to whether total surveillance by the state ever could be justified, and if so under what conditions. Would, for example, and notwithstanding the earlier challenge to a simplistic dichotomy between security and privacy, the guarantee of a genuinely crime-free society justify the surveillance of every aspect of our lives? I suspect not.

Social welfare is one of the subjects which traditionally receives far less attention from scholars than those of the preceding chapters. Yet it is an area steeped in surveillance practices, from the taking of censuses to the provision of health and social care at the expense of the state. Those who seek such care are subject to far greater levels of state surveillance than their more fortunate fellow citizens. This surveillance may be variously justified as care for the needy or detection of the greedy, depending on whom the appeal is made to. Whether either of these justifications really holds, though, is a different matter. What of public duties to share data for the general good? This has hit home particularly in the wake of COVID-19 where infection rates can be traced and people suspected of infection can be alerted to self-quarantine, thanks to surveillance through mobile phone applications. However, does one have a duty to download and use such an app (Klar & Lanzerath, 2020)? Is refusal to do so a civil right or a breaking of the social contract?

Surveillance in the private, as opposed to the public, sphere tends to be far less regulated and, as a result, far more ethically complex in its execution. This is particularly so in the case of corporate espionage, which may range from stealing items from bins outside a company's headquarters to paying for privately owned spy satellites taking images of competitors' facilities to determine activities through the number of cars in the corporate parking lot (Javers, 2010). Whether any of these activities are necessary in themselves is contentious to say the least, but what of counter-espionage? When a company suspects that it is subject to espionage, is it justified then in engaging in surveillance to limit the damage of lost company secrets? A possibly less contentious area is the surveillance of potential senior hires, looking at those moving into salaried positions worth millions. Such people will generally know that they are going to be subject to some level of surveillance to ensure that they are not quietly taking drugs or sleeping with prostitutes, or other activities which might bring the hiring company into disrepute. But when should such surveillance end? Can it extend to a school soccer fixture on a Saturday afternoon, or to family outings? Here there are clearly proportionality considerations to be borne in mind, but these will depend on the value placed on the wrongs visited on the innocent family members.

Not all private surveillance is as dubious as corporate espionage, but it may raise serious ethical questions, nonetheless. There are, for instance, commercial uses of surveillance such as targeting advertising in order that the return on investment of an advertising campaign can be maximised. This has been the financial model of many social networks in the second and third decades of the twenty-first century, but has also led to the targeting (and micro-targeting) of political advertising, which would not have been possible in the twentieth century (see various chapters in Macnish & Galliott, 2020). Even without the political angle, is such advertising a welcome democratisation of the personal service once restricted to the elite, or is it a weak facsimile, seducing someone to serve the interests of the corporate world? As with questions of state security mass surveillance and public health concerns, the relatively new development of 'big' data analytics has introduced new challenges to our understanding of how our information is collected and used by corporations.

Journalism may seem a more obviously justified form of surveillance than corporate or commercial surveillance. However, the ethics of journalism is itself a richly contested field of discourse, and much of this touches on the surveillance practices of journalists themselves. While political exposés such as that of Watergate seem clearly to be in the public interest, could this extend to journalists monitoring politicians 'just in case' they do something wrong, subjecting them to total surveillance (Lawlor & Macnish, 2019)? In such cases, who is it that gets to determine what is 'wrong'? This would seem to have been the behaviour of the *News of the World* and other newspapers in the UK in the wake of the hacking scandal in 2011. Related to the hacking scandal was also the question of fishing expeditions, a claim that was raised throughout the subsequent enquiry without ever being clearly defined. This chapter provides an analytic breakdown of the different uses of the term 'fishing expedition' to understand what it means and why each differing instance may be wrong.

Private investigators are subject to even less academic ethical reflection than corporate espionage, and yet, particularly in the USA, private investigation is a significant industry which supports the legal profession in investigating crimes, employers in identifying false claims of injury, and spouses suspicious of their partner's fidelity. To classify all these together would be a blunt response to a legitimate profession, albeit one that is under-regulated and therefore prone to unethical practices by some. Here questions arise regarding honesty, and the temptation for the private investigator to pretend to be someone they are not, so as to elicit information, and the practice of entrapment. This last involves the investigator flirting with the subject under suspicion to determine whether he (and it is more often a man) is faithful to his partner. Many are sceptical of this approach, but the chapter digs into why this is an unethical practice.

The last chapter on private surveillance is one that has touched many in the year of COVID-19: surveillance in the workplace by employers. With multiple lockdowns and the increase in working from home, this has extended from the office or factory to the home study, spare bedroom, or any place where a laptop can be balanced. There are companies that can offer employers software to log keystrokes and even take pictures of employees at regular intervals to ensure that they are at their desk and focussed on the monitor. This seems to be clearly excessive, but what of employers' duty of care for their staff? Employers may argue that they can only help with health and safety conditions 'at work' through surveillance techniques when the work is being carried out in the home. Even in the office, though, or on the road for drivers being monitored, it does not follow that employees should have no expectation of privacy. If they have a reasonable expectation of privacy in company toilets, then it does not follow that once off company property that expectation ceases. Instead, careful, and nuanced reflection is required to determine whether, where, and when such surveillance could be justified.

While the second, applied part of the book focusses on the public sector and the private sector, the last two chapters expand out to look at surveillance in public spaces and surveillance in family and other care situations. As to the former, it may be asserted by some that there is no reasonable expectation of privacy in public. However, this has not always been the view of the US Supreme Court, which has ruled that surveillance of public telephones and tracking devices placed on private vehicles driven on public roads are both breaches of the Fourth Amendment to the US Constitution, guaranteeing citizens' freedom from search and seizure (*Katz* v. *United States*, 1967; *United States* v. *Jones*, 2012). Even without appeal to judicial authority, we would feel it wrong if it transpired that someone had hidden a microphone in a park bench to record conversations. How much difference is there between that and the increasingly ubiquitous presence of CCTV and automated number plate recognition systems? What of cases in which communities (typically non-white) have been subject to so-called 'rings of steel' whereby no one can enter or leave the community on foot or by car without being registered by a camera? Facial recognition systems have been a further development on these technologies, resulting in similarly discriminatory practices (Hill, 2020).

The final chapter considers surveillance at the two ends of life, providing some further insight into why we may object so viscerally to surveillance in at least some contexts. As infants, we are subject to surveillance by our parents and communities and rightly so: to do otherwise would be negligent on their part. As we grow in independence, so we expect to be subject to diminishing surveillance from our parents as a sign of trust and adulthood. Hence, a return to childhood levels of surveillance may feel infantilising to the extent that we may start to act in a less responsible manner. This also makes it troubling when we age and enter end-of-life care, which may also employ surveillance practices, ostensibly for our care and benefit, but potentially also for the security of staff and of residents. More than this, though, to what degree do those of us not yet at this stage of life tend to assume that age implies a decline in cognitive abilities and autonomy, thus justifying the very surveillance that we would reject in our own lives? There is a risk that we use age as a proxy for incapacity in a way that is demeaning and leads to harm to the elderly in society.

CONCLUSION

In summary, this work is an attempt to introduce the key ethical questions and discussions surrounding many areas of surveillance practice and theory. While not comprehensive, its goal is to be both accessible and rigorous. As with much philosophical writing, it tends to ask more questions than it answers. At the same time, it does provide a solid and balanced overview of those issues which should prove helpful for those seeking guidance and this introduction helps steer the chapters in the following collection towards addressing substantively a selection of these key concerns.

REFERENCES

Ball, K., Lyon, D., Murakami Wood, D., Norris, C., & Raab, C. (2006). *A report on the surveillance society*. Produced for the Information Commissioner by the Surveillance Studies Network. Information Commissioner's Office, London.

Bellaby, R. W. (2014). *The ethics of intelligence: A new framework*. London: Routledge.

Doyle, T. (2009). Privacy and perfect voyeurism. *Ethics and Information Technology*, *11*, 181–189.

Hill, K. (2020). Facial Recognition Tool Led to Black Man's Arrest. It Was Wrong. *The New York Times*, June 25, 2020, Section A, Page 1 (New York edition).

Javers, E. (2010). *Broker, trader, lawyer, spy: The secret world of corporate espionage* (1st ed.). New York, NY: Collins Business.

Katz v. *United States* (1967). U.S.

Klar, R., & Lanzerath, D. (2020). The ethics of COVID-19 tracking apps – Challenges and voluntariness. *Research Ethics*, *16*, 1–9.

Lawlor, R., & Macnish, K. (2019). Protecting politicians' privacy for the sake of democracy. In C. Fox & J. Saunders (Eds.), *Media ethics, free speech, and the requirements of democracy*. New York, NY: Routledge.

Lyon, D. (2007). *Surveillance studies: An overview* (1st ed.). Cambridge: Polity Press.

Macnish, K. (2014). Just surveillance? Towards a normative theory of surveillance. *Surveillance and Society*, *12*, 142–153.

Macnish, K. (2016). Persons, personhood and proportionality: building on a just war approach to intelligence ethics. In J. Galliott, W. Reed (Eds.), *Ethics and the future of spying: Technology, national security and intelligence collection* (pp. 111–122). New York, NY: Routledge.

Macnish, K. (2018). *The ethics of surveillance: An introduction* (1st ed.). London: Routledge.
Macnish, K., & Galliott, J. (Eds.). (2020). *Big data and democracy*. Edinburgh: Edinburgh University Press.
Nathan, C. (2017). Liability to deception and manipulation: The ethics of undercover policing. *Journal of Applied Philosophy*, *34*, 370–388. https://doi.org/10.1111/japp.12243
Omand, D. (2012). *Securing the state*. London: Hurst.
Quinlan, M. (2007). Just intelligence: Prolegomena to an ethical theory. *Intelligence and National Security*, *22*, 1–13.
United States v. *Jones* (2012).
Wertheimer, A. (2006). *Coercion*. Princeton, NJ: Princeton University Press.
Wertheimer, A. (1999). *Exploitation* (New ed.). Princeton, NJ: Princeton University Press.