12. From 'need to share' to 'need to care': information aggregation and the need to care about how surveillance technologies are used for counter-terrorism

Adam Henschke

1. INTRODUCTION

Imagine this scenario: Anne, a soldier on deployment at a military base in a foreign conflict, meets a friend, Barry, for their morning jog. She posts, before and after, selfies of herself and Barry, updates her 'JoggerLogger' social media account with details of her run, and then heads to the shower. In doing this, Anne has put counter-terrorism operations at risk. The underpinning problem is that Anne has not treated potentially important information with due care. This chapter argues that individuals need to be careful with their personal information and that of others, even if that information is publicly available and/or relatively innocuous. Ultimately, I suggest that we need to shift our attitude to personal information from 'need to share' to 'need to care'.

To explain, let us start with the shower. While taking a shower in and of itself is hardly a cause for alarm, in this scenario, Anne is using a shower with a heating system that is linked to a 'smart meter'. To reduce energy use on the base, smart meters are being linked to smart grids to identify and anticipate peaks and lulls in energy use (Zhou et al. 2016). Every time the shower is used, the smart meter collects and communicates that spike of use. Recognizing that energy spike – and information on its timing, intensity and duration – can lead an external observer to infer that someone is taking a shower. Unfortunately, this smart meter was sold by a vendor who not only retained the default passwords (Chapman and Uren 2018; Kan 2016; Pishva 2016), but also had such poor cybersecurity practices that anyone with minimal cyber skills could find those passwords (Chapman and Uren 2018); thus, attackers are able to hack into the smart meter's communications to gather information on use, and to

analyse the information for patterns. The smart meter gives the hacker information that forms a picture of the patterns of the base's life. For those wishing to understand the movements within a military base, the times when people shower can provide useful data for when to plan attacks, and when those on the base might be preparing for their own offensive operations. The point is that this new technology creates new opportunities for innocuous data to be gathered and analysed in ways that reveal sensitive information.

Anne's second mistake was taking selfies with Barry and posting them to her social media account. While photos of the two of them are great for friends and families to see, unbeknown to Anne, Barry is often involved in recruiting foreign assets for counter-terrorism Intelligence work. Being a uniformed soldier, Anne obviously has no concern about being identified as part of the military, but Barry has to be more careful. The problem here comes from the decline in price, ease of access and increased power of artificial intelligence (AI) to power facial recognition technology (FRT). Consider that an enemy Intelligence operative sees Anne in her uniform and takes a series of photos of her. FRT is used to identify her face, and AI is then used to trawl social media for her face. Every time another person comes up in Anne's photos, their face is identified and flagged as an associate. Barry is now flagged as an associate of Anne's, and his actions are put under closer attention. This makes Barry's counter-terrorism job much harder and potentially puts any locals Barry is seeking to recruit to the counter-terrorism operation at risk. Since he started working in counter-terrorism, Barry has been careful about his personal information, but old social media posts are found from the military training he did fifteen years ago. There are a number of photos of Barry and his friend, Claire, who trained together. Through FRT, Claire's face comes up in old photos. Unfortunately, Claire is currently running a secret counter-terrorism operation under a fake identity. This operation and Claire's life are now at risk. The new technologies pose a real risk to effectiveness, operational security and individual safety.

Finally, there is Anne's JoggerLogger. This is an imaginary brand of a wearable technology that monitors Anne's heart rate and other personal vitals, as well as locating her jogging times and routes. Being a social networking company, JoggerLogger posts all this information to the JoggerLogger community for them to compare and motivate each other to be their best. Problematically, this particular technology and company are big supporters of national security, and give a 50% discount to active military, police and other national security employees, meaning that it is the favoured device and platform of members of these communities. As such, a canny observer can guess where groups of military, police and national security people are located by identifying clusters of joggers on the JoggerLogger global map. The point here

is that certain technologies and their integration with social media can become uniquely sensitive if a particular pattern of use or user is identified.

None of this should be at all surprising. That we can induct something like shower use from other information, such as spikes in energy use, is hardly a shock. Likewise, the concerns of security officials about social media and its impacts on undercover operations have been publicly discussed since at least 2015 (Lord 2015). The JoggerLogger example is slightly adapted from a case in 2017. In this case, a wearable device associated with jogging was connected to the Internet, uploading the data to a publicly accessible website, Strava. The fitness-tracking app revealed potentially sensitive information about military bases and supply routes via its global heat map website. The data map shows one billion activities and three trillion points of latitude and longitude from 'Strava's global network of athletes…according to the American company… Using satellite imagery, you can see base buildings, for example. But on the heat map, you can see which buildings are most used, or the jogging routes of soldiers' (Bogle 2018). This security weakness was not particularly complex and was exposed by a master's student.

What is new and relevant here are the technologies, what they can reveal through the aggregation of seemingly innocuous information, and the pressure they put on how we understand and treat personal information. Because these technologies lead to a capacity for aggregation of innocuous information, this creates problems morally and for counter-terrorism. In this chapter, I promote the general idea that information – particularly innocuous information – should be treated with care. I offer the conceptual mechanics that underpin this claim.

2. SHIFTING RELATIONS TO INFORMATION: FROM 'NEED TO KNOW' TO 'NEED TO SHARE'

Until late 2001, in the US and elsewhere, national security agencies followed a general rule in the way they treated sensitive information: one only got access to it on a 'need-to-know' basis. As a US Congressional Research Service report puts it: 'The basic approach taken by the U.S. Government has been focused on establishing "need-to-know." Sensitive information is made available only to those persons with appropriate clearances and a "need-to-know" that information for the performance of their duties' (Best 2011).

Then, on 11 September 2001, the US suffered its worst domestic terrorist attack, and their national security infrastructure changed. As came to light, many of those who hijacked the planes were on various watch lists (National Commission on Terrorist Attacks Upon the United States 2004, pp. 83–4). The question then became, if the state knew that these people posed a threat, how did they slip through the net? One of the key conclusions drawn from the 9/11 investigation was that, though some arms of the US national security

apparatus knew about these potential threats, this information was not shared with its other arms. A key weakness was identified – that information relevant to national security was not being effectively shared across the vast body of national security agencies in the US: 'In the aftermath of the 9/11 attacks in 2001, a consensus emerged that information sharing, especially between Intelligence offices and law enforcement officials had been deficient and had contributed to the failure to detect the plot in advance' (Best 2011).

'Need to know' had prevented internal sharing of information. Because of the 9/11 attacks, there was a deliberate internal shift in the ways that sensitive information was to be treated. 'Need to know' was no longer the default. The US shifted its position from 'need to know' to 'need to share' (Best 2011). Responding directly to Intelligence failures brought about by information restriction, the default position became more active sharing of information. In parallel, by 2017, more than four million people in the US were eligible to access confidential, secret or top-secret information (Office of the Director of National Intelligence 2017). After the 9/11 attacks, the national security community saw a 'need to share' more information more freely to prevent another such attack from occurring. According to Genevieve Lester (2016), this sort of shift is common in Intelligence practices – there is a pendulum that swings between increased oversight and constraint and greater scope for freedom and power following tragedies (pp. 162–63). Following the 9/11 attacks, more information was being shared by more people more easily.

Parallel to these changes in attitude in the Intelligence communities, we have seen a similar attitudinal shift in the public at large. Many of us now actively and willingly share vast amounts of personal information on social media:

> What marks this age as one of *surveillance* is our own role in this – it is not simply that there are new information technologies…we are often the willing sources of this information, happily uploading selfies, buying wearable surveillance technologies, actively publicising [p]ersonal [i]nformation like no other time in history. (Henschke 2017, p. 4, emphasis in original)

Moreover, those social media and information companies have led to the development of so-called 'surveillance capitalism', where private companies make billions of dollars through the information that we provide to them (Zuboff 2019). We now place so much personal information into the public realm that the information once collected by police states seems quaint. Moreover, any claims to privacy seem confused if we are the active sources of the information (Henschke 2017). In short, individuals' behaviour and the modern economy are all evidence of a widespread attitude that we 'need to share' our personal information.

Given these institutional and social shifts towards massive sharing of personal information, often in public spaces, what does this mean for practices like counter-terrorism surveillance? One inference made by some is that privacy is dead – there is so much personal information 'out there' that we need no longer worry about adhering to privacy. Another upshot is that those working in national security sectors like counter-terrorism need to take better care with their own personal information. However, as we look at different notions of privacy, we will see that the first implication is conceptually muddled. Moreover, as we look at the revelational powers of these new technologies, we will see that, not only do those working in areas like counter-terrorism need to take better care with their own information, but they also need to take more care with other people's information.

3. RETHINKING PRIVACY[1]

The technological challenge to notions of privacy is central to the discussion and requires us to engage with the tight relation between privacy and technology. The liberal-democratic concept of privacy was crystallized in the seminal paper 'The Right to Privacy', written by Samuel Warren and Louis Brandeis in 1890 (Warren and Brandeis 1890). Importantly, this concept was developed *in response* to new technologies: 'In the late 19th century cameras had become portable, could take photographs practically in an instant and could be used by almost anyone who could afford one. Foreshadowing current debates about surveillance technologies, Warren and Brandeis were concerned about the ways that new technologies invaded personal space' (Henschke 2017, p. 35). This 'new [photographic] technology made it important to explicitly and separately recognize this protection under the name of privacy' (DeCew 2006). In the liberal-democratic tradition, at least, technology and privacy have had a close relationship with modern notions of privacy being developed *in response* to new technologies. The point is that we should not assume that new technologies necessarily mean the death of privacy.

To make sense of this claim that privacy is still very much alive, we need to understand what privacy refers to. A common way to think of privacy is as something secret. This notion of privacy-as-secrecy takes its roots in ancient Greek thought, where a binary distinction was made between political and domestic life, the *polis* and *oikos* (Arendt 1958, p. 24). This binary, where privacy is understood in contrast to the public, leads to what Daniel Solove calls 'the secrecy paradigm': 'Under this view, privacy is violated by the public disclosure of previously concealed information' (Solove 2008, p. 21). Importantly, when privacy is understood as secrecy, 'when others know the information, it is no longer completely secret' (Solove 2008, p. 139). Thus, if a person willingly places personal information into the public sphere, it seems

strange for them to claim that people ought to respect their privacy. Likewise, once something is publicly accessible, it is no longer private, and so – on a simplistic application of the secrecy paradigm – that information is no longer afforded the protections of privacy.

However, privacy is more than simply secrecy. When thinking of it in a political sense, privacy is seen as the opposite to government intrusion: the private describes that zone that the government is not permitted to interfere in (Henschke 2020). Continuing this political frame, privacy might be thought of as an instrumental good, something necessary for democratic freedom (Greenwald 2014, p. 177). Taking it from the explicitly political, we might instead think of privacy as a space of non-interference. Privacy 'is a set of boundaries we create between ourselves and others' (Solove 2008, p. 74). We can also think of privacy as control, specifically, 'the control we have over information about ourselves' (Fried 1969, p. 482). Here, privacy draws from the recognition that an individual has some legitimate claim to control their personal information. Another view suggests that, while 'control' is morally important, privacy is better understood as being concerned with access (Macnish 2018).

More recent accounts take pluralistic approaches, arguing that we think of privacy in different terms, such as data protection (van den Hoven 1999), or 'context-relative informational norms' (CRINs) (Nissenbaum 2009), or that privacy is a bundle of related concepts (Henschke 2017, pp. 28–55). The data protection account seeks to avoid unnecessary conceptual debates about what privacy *is*, and instead focuses on the *ends* of privacy: it asks what privacy is actually doing for us and why access to information should be constrained (van den Hoven 2007, p. 320) by identifying four moral justifications for protecting data: '1) Information-based harm; 2) Informational inequality; 3) Informational injustice; and 4) Encroachment on moral autonomy' (van den Hoven 2007, p. 320). In a similar line of reasoning, Helen Nissenbaum argues that we should respond to privacy concerns not by reference to some particular conception of privacy, but instead we should be concerned with determining appropriate information flows. 'Usually, when we mind that information about us is shared, we mind not simply that it is being shared but that it is shared in the wrong ways and with inappropriate others' (Nissenbaum 2009, p. 142). She looks at CRINs: these are 'characterized by four key parameters: contexts, actors, attributes and transmission principles' (Nissenbaum 2009, p. 140). In other writing, I have suggested that we need to see both descriptive and normative concepts play a role in a broader pluralistic idea conception of privacy (Henschke 2017, pp. 28–55).

This list is not exhaustive.[2] It does not claim to capture all the myriad concepts of privacy and their interactions.[3] Moreover, it does not aim to resolve which of these concepts is the correct one – quite the contrary. Part of the

problem with our current understanding of privacy is a search for the correct concept. Consider the opening paragraph from Julie Inness's (1992) *Privacy, Intimacy, and Isolation*:

> Exploring the concept of privacy resembles exploring an unknown swamp. We start on firm ground, noting the common usage of 'privacy' in everyday conversation and legal argument. We find intense disagreement about both trivial and crucial issues... we find chaos...the ground starts to soften as we discover the confusion underlying our privacy intuitions. (p. 3)

My point here is twofold. First, we need to recognize that there are a range of ways that we can understand privacy, and these extend far beyond seeing privacy simply as secrecy. Thus, we have a range of conceptual tools at our disposal to understand and apply to the production, collection and use of personal information. Second, just as national security communities changed their attitudes to information following the 2001 attacks, as technologies and our behaviours continue to evolve, we need to change attitudes to personal information again.

One way to start this attitudinal shift is to think of personal information as being concerned not just with what is in public or private, or even who controls or has access to the given information, but whether that information is intimate, or from a terrorism/counter-terrorism perspective, sensitive. Under a conception where privacy is concerned with intimacy, the starting point is the relation that an individual has to certain personal information. Specifically, an intimacy account holds that what is of relevance is a person's attitudinal stance – that they like, love or care about particular information:

> When an agent characterizes an act or activity as intimate, she is claiming that it draws its meaning and value from her love, liking or care. Intimate decisions concern such matters and, thus, involve a choice on the agent's part about how to (or not to) embody her love, liking or care. (Inness 1992, pp. 74–5)

On Inness's account, privacy is an attitudinal state whereby those decisions, actions or facts about a person which they love, like or care about are what is of interest.

I suggest here that national security communities take a similar approach to information – they recognize that certain information is *sensitive* and ought to be treated in a particular way because of that sensitivity. The basic idea of sensitivity is that, due to the importance of information for reasons such as national security, Intelligence or that it is relevant to an ongoing counter-terrorism operation and so on, those tasked with using or controlling access to that information now have a particular attitudinal stance towards it. Information deemed sensitive in a national security context is often classified

as confidential, secret, top secret and so on. As a result of these classifications, those working with it treat that information with due care, and have a set of processes in place to ensure that it continues to be treated with due care.

The public/private distinction and notions of secrecy are not of primary concern here; what is of importance is our attitude to that information, and how that attitude shapes our access to, and use of, that information. This notion of caring for information, showing the proper attitude towards information that recognizes it might be intimate or sensitive, is not just relevant in a general moral sense but for counter-terrorism practices as well (see below). However, we need to make one more step before we can see why personal information, particularly seemingly innocuous personal information, needs to be treated with care.

4. ANALYTICS AND REVELATION

The claim that we ought to treat certain information as intimate (when in a personal context) or sensitive (when in a national security context) with due care may be obvious. However, given the power of information technologies to collect and analyse vast amounts of information to produce new and increasingly intimate and sensitive information, we need to treat seemingly innocuous information with care. Consider that a teenage girl buys the following items: cocoa-butter lotion, a large purse, vitamin supplements (zinc and magnesium) and a bright blue rug. Now imagine that the girl's family subsequently receives a package in the mail congratulating her on becoming pregnant. The company, Target, did this. They had been using data analytics to reveal useful information about their customers, such as their 'pregnancy score' (Hill 2012). The point here is that what seems like mundane information when analysed can be particularly revealing. It can expose or uncover things about a person that are particularly intimate or sensitive, despite the initial information being innocuous or mundane.

This is the key observation from the opening example about Anne posting selfies, using wearable technology that communicates her actions with social media and using a smart-metered shower: each of these actions and the information they produce alone are innocuous and mundane. However, when particular technologies are applied to those actions, sensitive information can be produced or revealed. As I have argued elsewhere, the aggregation and analysis of innocuous information can reveal intimate and sensitive information, and can create new information from that mundane information that is highly revealing (Henschke 2017, pp. 144–49). The point is that, due to the revelational power of these new technologies, we need to treat even innocuous and mundane information – given it is aggregated and analysed – with increased care.

The concern is that in assessing data points independently of each other, we make a 'mistake in our moral mathematics' (Parfit 1987, pp. 67–86). The moral importance of a particular action is undervalued as a result of considering it independently:

> It is not enough to ask, 'Will my act harm other people?' Even if the answer is No, my act may still be wrong because of its effects. The effects that it will have when it is considered on its own may not be its only relevant effects. I should ask, 'Will my act be one of a set of acts that will *together* harm other people?' The answer may be Yes. And the harm to others may be great. If this is so, I may be acting very wrongly. (Parfit 1987, p. 86, emphasis in original)

Given the increased ubiquity of information technologies, and their increased capacities to analyse and reveal sensitive information, what we need to ask is *whether the sets of data together* will harm other people. Purchasing cocoa butter is of almost no consequence. Being pregnant is not. Taking a shower is largely irrelevant. The behavioural patterns that it generates can reveal militarily sensitive information, which is highly important in a conflict zone. This is the core recognition of the shift from 'need to know' to 'need to share': we gain new information by the aggregation of existing information, and our attitudes also need to shift.

The power of sharing information comes from the ways in which information analytics lead to revelation. Through aggregation and analysis, new information is revealed and produced (Henschke 2017, pp. 126–51). Like the difference between a jigsaw puzzle before and after completion, aggregation and analysis afford a whole portrait to emerge. The power of analytics comes from converting the innocuous to the intimate, revelation of the profound from the mundane. What was largely irrelevant, in combination and following analysis, can become highly sensitive.

Combining this capacity for revelation with the conceptualization of privacy-as-secrecy, we ought to now be able to recognize the core point of this chapter: individual data points are innocuous, and their location in the public realm means that they are no longer secret. So why should we care about them? First, they can be easily aggregated and analysed to reveal intimate and sensitive information. Second, that because this information is sensitive – that is, could be detrimental to national security and so on – if it gets into the wrong hands, means that it ought to be cared about. As we saw, privacy is more than secrecy, so whether that sensitive information is in the public sphere is irrelevant. What is relevant is what it reveals, and we ought to treat it as important. Maybe one could claim that we always need to have a duty of care in relation to confidential information, however, the problem is that the potential for aggregation and analysis means that there is a need for a duty of care in relation to information in the public domain because it can be aggregated and analysed

in ways that enable harm. In short, we need to shift from 'need to share' to 'need to care'.

5. THE 'NEED TO CARE' FOR INFORMATION AND ITS IMPLICATIONS FOR COUNTER-TERRORISM

As with the shift in attitude from 'need to know' to 'need to share', I am suggesting that we should now make further changes in our treatment of personal information. Seeing privacy beyond the secrecy paradigm encourages an attitudinal shift to the way personal information is treated. Our attitudes should shift from 'need to share' to 'need to care'. We now have a theoretical apparatus to explain why we need to treat information with care: innocuous information is potentially revelational if aggregated and analysed. Insofar as what is revealed may be intimate or sensitive is something of moral and practical importance, it follows that we need to treat information with due care. In short, we can see that information, even if it is accessible and thus not secret, can and should be considered private and so ought to be treated carefully.

There are four general implications of this shift to 'need to care'. As said, the point is that we need to change our attitudes towards information, recognizing that innocuous information can be intimate and sensitive. For individuals, the first implication is that we take care with how information about *us* is collected, produced and used. Such a demand applies to what *we* post online, and what we allow companies and even governments to do with that information. Insofar as we are concerned about others treating information with care, we ought to be careful with information about ourselves that we make public.

The second implication for individuals arises from basic consistency – if we generally do not want others to access and use intimate information about us, then we ought not access and use intimate information about them. That is, we 'need to care' for their information, even if it is in public. Privacy, on a complex pluralistic notion, holds us to consider that innocuous information, even if it is about other people, is still due respect. Again, our attitudes need to shift such that even shared information is treated with care.

The third implication applies to those in the national security and counter-terrorism space. Because innocuous information can reveal sensitive information, those in the counter-terrorism space need to be careful with their own information. The opening example about Anne took a range of technologies to show how standard public sharing behaviours can pose national security risks and can undermine counter-terrorism efforts. The point, again, is that those involved in these areas and operations need to take special care with information. Normal sharing behaviours, such as taking and posting selfies, using wearable exercise devices and so on, need to be revisited when

in a context like counter-terrorism. This responsibility to care for information also applies to issues like procurement – one of the security vulnerabilities identified stemmed from the lack of effective security on smart meters for showers. The responsibility here is for those involved in things like logistics, procurement and so on to be particularly careful about the security vulnerabilities that can arise from innocuous information.

The final point is that, just as individuals need to take more care with what sorts of public information they access, so too do national security and counter-terrorism operations need to treat publicly available information with due care. The point is not to say that counter-terrorism operations that engage in surveillance are unjustified – given certain national security threats, privacy can be overridden. Rather, the point of shifting to 'need to care' is to show that justifications are still needed even when accessing publicly available information or innocuous information. State surveillance programs, even those that use publicly accessible information, require justification and independent oversight. Warranting processes, for instance, might be a way of ensuring that this information is treated with due care. As a guiding principle, the 'need to care' rule makes those working with personal information, particularly those working with innocuous personal information and/or publicly available information, see that such information still deserves to be seen as private.

6. CONCLUSION

To conclude, public information might still be considered under the umbrella of privacy, and innocuous information can be highly revealing. These points are vital to recognize as the revelational power of analytics, coupled with the ubiquity of surveillance technologies and pervasiveness of publicized behaviours, means that we are drowning in innocuous information. Yet, despite this information not being secret, we need to take care with how we treat it. Recognizing the plurality of privacy concepts allows us to think beyond the secrecy paradigm; seeing that personal information can be intimate or sensitive signals to those involved in national security that the information needs to be treated with due care. In short, we need to shift attitudes from 'need to share' to 'need to care'.

NOTES

1. This section draws from 'On Privacy', in *Ethics in an Age of Surveillance* (Henschke 2017, pp. 28–55).
2. Judith DeCew's (2006) privacy entry in the *Stanford Encyclopedia of Philosophy*, Daniel Solove (2008) and Helen Nissenbaum (2009) all give great overviews of the range of privacy conceptions.
3. See Koops et al. (2016) for more on this.

REFERENCES

Arendt, Hannah (1958), *The Human Condition, Charles R. Walgreen Foundation Lectures*, Chicago: University Of Chicago Press.

Best Jr., Richard A. (2011), *Intelligence Information: Need-to-Know vs. Need-to-Share*, Washington, DC: Congressional Research Service.

Bogle, Ariel (2018), 'Strava Has Published Details about Secret Military Bases, and an Australian Was the First to Know', ABC News, 30 January 2018, http://www.abc.net.au/news/science/2018-01-29/strava-heat-map-shows-military-bases-and-supply-routes/9369490.

Chapman, Eliza, and Tom Uren (2018), *The Internet of Insecure Things*, Canberra: Australian Strategic Policy Institute.

DeCew, Judith (2006), 'Privacy', *Stanford Encyclopedia of Philosophy*, accessed 19 September 2007 at http://plato.stanford.edu/archives/fall2006/entries/privacy/.

Fried, Charles (1969), 'Privacy', *Yale Law Journal* 77 (3), 475–93.

Greenwald, Glenn (2014), *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York: Metropolitan Books.

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

Henschke, Adam (2020), 'Privacy, the Internet of Things and State Surveillance – Handling Personal Information within an Inhuman System', *Moral Philosophy and Politics* 7 (1), 123–49.

Hill, Kashmir (2012), 'How Target Figured Out a Teen Girl Was Pregnant before Her Father Did', *Forbes*, 16 February 2012, accessed 11 January 2016 at http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

Inness, Julie C. (1992), *Privacy, Intimacy, and Isolation*, New York: Oxford University Press.

Kan, Michael (2016), 'IoT Botnet Highlights the Dangers of Default Passwords', *InfoWorld*, 4 October 2016.

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chokrevski, and Masa Galic (2016), 'A Typology of Privacy', *University of Pennsylvania Journal of International Law* 38(2), 483–575.

Lester, Genevieve (2016), *When Should State Secrets Stay Secret?*, Cambridge: Cambridge University Press.

Lord, Jonathan (2015), 'Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age', *International Journal of Intelligence and CounterIntelligence* 28 (4), 666–91, doi: 10.1080/08850607.2015.1022464.

Macnish, Kevin (2018), 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World', *Journal of Applied Philosophy* 35 (2), 417–32.

National Commission on Terrorist Attacks Upon the United States (2004), *Final Report of the National Commission on Terrorist Attacks Upon the United States*, Washington, DC: Government Printing Office.

Nissenbaum, Helen (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, CA: Stanford Law Books.

Office of the Director of National Intelligence (2017), *Fiscal Year 2017 Annual Report on Security Clearance Determinations*, Washington, DC: National Counterintelligence and Security Center.

Parfit, Derek (1987), *Reasons and Persons*, Oxford: Oxford University Press.

Pishva, Davar (2016), 'Internet of Things: Security and Privacy Issues and Possible Solution', *ICACT Transactions on Advanced Communications Technology* 5 (2), 797–808.
Solove, Daniel (2008), *Understanding Privacy*, Cambridge, MA: Harvard University Press.
van den Hoven, Jeroen (1999), 'Privacy and the Varieties of Informational Wrongdoing', *Australian Journal of Professional and Applied Ethics* 1 (1), 30–43.
van den Hoven, Jeroen (2007), 'Privacy and the Varieties of Informational Wrongdoing', in John Weckert (ed.), *Computer Ethics*, Aldershot: Ashgate Publishing, pp. 317–30.
Warren, Samuel D., and Louis D. Brandeis (1890), 'The Right to Privacy', *Harvard Law Review* 4 (5), 193–220.
Zhou, Bin, Wentao Li, Ka Wing Chan, Yijia Cao, Yonghong Kuang, Xi Liu, and Xiong Wang (2016), 'Smart Home Energy Management Systems: Concept, Configurations, and Scheduling Strategies', *Renewable and Sustainable Energy Reviews* 61, 30–40, doi: 10.1016/j.rser.2016.03.047.
Zuboff, Shoshana (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London: Public Affairs.