Adam Henschke*

Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System

https://doi.org/10.1515/mopp-2019-0056

Abstract: The Internet of Things (IoT) is, in part, an information handling system that can remove humans from the information handling process. The particular problem explored is how we are to understand privacy when considering informational systems that handle personal information in ways that impact people's lives when there is no human operator in direct contact with that personal information. I argue that these new technologies need to take concepts like privacy into account, but also, that we ought also to take these technologies into account to reconsider and perhaps reconceptualise privacy. This paper argues that while an inhuman system like the IoT does not necessarily violate the *interpersonal* privacy of people, if the IoT is used as part of a state surveillance program, a *political* notion of privacy may be violated.

Keywords: privacy, applied ethics, internet of things, surveillance, privacy as political, ethics of technology

1 Introduction

The particular problem that this paper explores is how we are to understand privacy when considering informational systems that handle personal information in ways that impact people's lives when there is no human operator in direct contact with that personal information. The Internet of Things (IoT) promises to usher in a series of explicit and implicit changes to our lives. These new technologies need to take concepts like privacy into account, but also, as per reflective equilibrium,[1] we ought also to take these technologies into

1 This approach to reflective equilibrium takes it that events in the world shape ethically loaded concepts like privacy as much as those concepts guide our behaviour. I mean here an approach like that described by Fritz Allhoff (2011), where 'neither the principles nor the judgments enjoy any sort of privileged role. Rather, they engage each other in a process of mutual revision'.

***Corresponding author: Adam Henschke,** Australian National University, 1 Lennox Avenue, Canberra, Australian Capital Territory, Australia, E-mail: adam.henschke@anu.edu.au

account to reconsider and perhaps reconceptualise privacy. This paper will argue that while an inhuman system like the IoT does not necessarily violate the interpersonal privacy of people, if the IoT is used as part of a state surveillance program, it does represent a morally concerning encroachment of state intrusion into the private spaces of citizens. The ultimate contribution of this paper is to show how different approaches to privacy respond to disruptive technologies and that a political account of privacy can explain concerns about these technologies.

New technologies like the IoT are often considered disruptive (Allenby 2013). Think of the myriad ways that the internet has disrupted our lives, laws and institutions. These disruptions also force us to rethink and revisit core concepts that we use to structure our lives. Again, consider the ways that the internet has put pressure on the concept of privacy. For some, the internet heralded a world without privacy (Hearn 2010). For others, however, the internet means that the traditional ways of thinking about privacy have given way to other concepts (Nissenbaum 2009; Solove 2008; van den Hoven 2008). Given the fact that so much of our lives are lived online now, rather than seeing privacy as secrecy (Solove 2008), for instance, we ought to think about privacy in the way that Jeffrey Reiman (1976) and Julie Inness (1992) suggested, as intimacy and care or to rethink privacy as a public notion, not just something that happens outside of public view as Helen Nissenbaum has suggested (2009). The point here is that changing circumstances in our world can make us reconsider key concepts that guide our behaviours, and the IoT represents a set of changes in our world that require us to consider and reflect on privacy.

The IoT refers to a cluster of technologies in which some combination of sensors, communication, actuators, and/or artificial intelligence are linked (Allhoff and Henschke 2018). The sensors are used to gather information about our world, which is then processed and communicated to other technologies. The actuators can then bring about some changes in the physical world, and the artificial intelligence acts to process the information and coordinate sensors, communications, and actuators. A standard example is Amazon Echo[2] when viewed as part of a larger complex integrated IoT system. The Echo device itself involves a microphone that listens for and processes user commands. If the user requests to purchase some product, that request is communicated to a central processing facility where the request is processed and converted to a physical

2 I make a distinction here between the Echo device and the Amazon Echo system. In this distinction, the *Echo* is simply the single appliance that listens for user commands, whereas the *Amazon Echo* refers to the integrated system that includes the Echo device but also refers to the larger integrated network that the Echo sits within.

expression such that the physical product is located, shipped, and delivered to the user (Whitney 2019; Connor 2019a, b). Importantly for this example, the Echo picks up on users' commands and, when the system is working seamlessly, the system goes through a series of functions such as ordering, locating, shipping, and delivering a product, without a human operator necessarily seeing, accessing, or handling any personal information.[3]

In this kind of process, because the human operator has been removed from the loop and there is no 'person' dealing with personal information, we must reconceptualise how we think of privacy and the elements attached to that ideal. When considering issues of state surveillance, the IoT poses particularly significant conceptual and ethical challenges. The reason is that the IoT can potentially allow for widespread state surveillance of citizens, but in a way that involves no human access to personal information. As we will see, the basic question is this: Does information that has no human contact still deserve privacy? If not, how should we treat the information gathered by the IoT? The IoT, being a set of disruptive techologies, forces us to reconsider basic concepts that shape and guide behaviour. However, a thoroughgoing ethical assessment of IoT will engage with and involve more than just privacy.

The paper proceeds as follows. It sets out the problem by looking at how IoT technologies will play an increasing role in surveillance and state surveillance in particular. It then looks at ways to conceptualise personal information and privacy to establish the ways that IoT disrupts our notions of privacy when considering state surveillance. The paper suggests that one conceptualisation of privacy as person-person relations would reject the notion that non-human information handling systems like the IoT necessarily invade our privacy. Instead, if we conceptualise privacy as state–citizen relations, we can accept the notion that non-human information handling systems like the IoT do invade privacy. I call these two approaches to privacy the interpersonal account and the political account, respectively. Thus, the paper concludes that, as the IoT can be both privacy respecting and privacy violating, in order to give a proper moral appraisal of disruptive technologies like the IoT, we need to see which actors are using the technologies and in which contexts.

The approach that I am taking here is therefore deliberately pluralistic. I mean this in two senses. First, I recognise that privacy itself is a pluralistic set of concepts (Henschke 2017a). A 'multi-dimensional model demonstrates the multi-faceted nature of privacy more sharply than just stating that privacy is "ambiguous" or "multi-faceted" – it shows what the main facets actually are that give particular colours to privacy in different situations' (Koops et al. 2016, p. 570).

3 I discuss the notion of personal information in section 3.

Second, my approach is pluralistic in that it suggests that interpersonal accounts and political accounts are *both* descriptively and normatively valuable. The issue that I explore is how inhuman systems show the different ways that the personal and political accounts treat information.

As Koop et al. note, 'privacy is notoriously hard to capture … The umbrella term *privacy* itself encompasses both the concept what privacy *is* and how it should be *valued* as well as a (generally) narrower *right to privacy* outlining the extent to which privacy is or ought to be legally protected' (Koops et al. 2016, p. 487, pp. 491 f., emphasis in original). To this end I don't seek to offer a description of privacy concepts. People like Koop et al. (2016), Daniel Solove (2006), and Helen Nissenbaum (2009) have done a good job of this. Like Koop et al., this paper's aim is 'not to define privacy or prescribe how we should understand privacy or what its relevance is; rather, the [paper] serves as an analytic tool that can assist in structuring and clarifying the privacy debate' (Koops et al. 2016, p. 489). My aim is to show that there are two parallel privacy accounts, interpersonal and political, and that inhuman informational systems may not be privacy violating in the interpersonal account, but may be violating in the political account.

2 The Internet of Things and State Surveillance

The IoT refers to a cluster of integrated informational and physical technologies that produce, access, process, and communicate information and act upon the physical world (Li et al. 2015). It is distinct from the 'internet', first as it is an interconnected set of 'things', and second as it typically involves things acting in the physical world. On the first point, the IoT is distinct from the internet in that it specifically involves sets of technologies that interact and communicate without necessarily having a human involved in key aspects of those communications. To start the discussion of state surveillance and the IoT, let us think of the IoT in the domestic context, the Amazon Echo. The *Echo* itself refers to the smart speaker–microphone device developed by Amazon. These speakers sit in the background and upon hearing the 'wake' word, typically the word 'Alexa', will respond to user commands. This system can be integrated with other devices in a smart home, allowing people to change room temperature, play music, order a pizza, book a car from a car sharing service, buy groceries etc.

When the Echo is working as intended, upon hearing the wake word, the user makes a request, and that request is carried out. When in a smart home, for instance, if a user requests that the Amazon Echo play a particular song, there is

no other human involved in the process. The user makes the request, the Amazon Echo system recognises what the request means in plain language, and fulfils the request. Note that the Amazon Echo system extends beyond the boundaries of a person's enabled smart home. A person can get a pizza delivered through a partner company like Pizza Hut, Dominos, and Papa John's (Connor 2019b), they can call a car from Uber (Connor 2019a), and they can order and buy groceries through Amazon Prime (Whitney 2019). While there are obviously people involved in these extended services – the Uber car still requires a driver – the information handling is all done automatically. That is, a set of technologies that are integrated through communications networks receive and analyse the user's requests, process the requests, and bring about some change in the physical world to deliver on the user's requests. I note here that Amazon has been heavily involved in research and development for drone delivery (D'Onfro 2019) and that Uber have been heavily involved in research and development for automated vehicles (Marshall 2019). And many delivery services like Amazon increasingly rely on automation and robots in their warehouses to fulfil an order. That is, it is possible in the near future that there will be no human operators needed to fulfil a person's request.

This is then a paradigm example of the IoT. We have a set of technologies, connected by communications networks, undertaking a range of tasks. While the initial request and current aspects of delivery rely on human users and operators, the vast majority of information handling is done by non-human 'things'. This presents the first significant difference between the IoT and the internet. While the internet is a complex technological communications system, the IoT differs in that it explicitly and necessarily relies on a set or network of linked things, and the communications between those things typically do not involve humans.

The second key difference between the internet and the IoT is that the IoT is a proper *cyber-physical system*. That is, communications between things involve *actuators* such that the IoT spans both informational and physical realms (Henschke 2017b). Consider a drone delivering a request from Amazon Echo. That request, while utilising information communications as part of the service, is not constrained to the informational realm. A product has to be identified in a warehouse and placed onto a drone. That drone then has to fly or drive to the relevant delivery address and deliver the ordered product. Unlike the internet, key functionalities here occurs in the physical realm.[4]

4 I have discussed elsewhere the conceptual and ethical issues arising from the IoT spanning both informational and physical realms (Allhoff and Henschke 2018; Henschke 2017b).

The IoT relates to state surveillance in two important ways. First, many of the IoT devices are designed to be largely invisible to us. Second, the responses allow for exercise of power in ways that are different from the ways in which state power is typically exercised. On the first point, the IoT can be seen as the ideal surveillance network. As many of the IoT devices will be small, silent, and largely ubiquitous, the IoT offers the opportunity to have large swathes of the population under surveillance at all times. Amazon Echo has already been involved in a criminal case in the US where prosecutors were seeking access to the Echo's request logs in order to help glean information on a case.[5] With the IoT, we have a surveillance network that can potentially monitor people in their homes, in their cars, in their workplaces, and in their cities. Moreover, this complex network of things is largely invisible to the users. The Amazon Echo sits quietly in a person's home, waiting to be activated by the given wake word. That means that the microphone is always on, potentially listening to any and all activities within the microphone's range. While Amazon do take pains to ensure constraints on what is listened to and when, many other IoT devices like smart TVs have been shown to listen to and observe people in their homes without their knowledge, much less their consent (Matyszczyk 2015).

Furthermore, the IoT adds a further complexity to surveillance as it is not just the single sensor-enabled devices that can act as surveillance devices, it is the network of things. The combination of a range of information sources produces virtual identities for information sources that can be highly revealing (Henschke 2017a). Consider if I had purchased cocoa-butter lotion, a large purse, vitamin supplements (zinc and magnesium), and a bright blue rug. Those purchases, when aggregated and analysed by the Target retail company told them that I had an 87% chance of being pregnant (Hill 2012). The point here is that modern information analysis technologies can convert innocuous information to highly revealing personal identities. Moreover, such revelations are not just the province of commercial actors. Consider the Cambridge Analytica controversy, in which people's social media identities were analysed to give an idea of their political inclinations and interests and then used as part of a political campaign (Knaus 2018; Lewis 2018). Like the pregnancy score, the power of social media for political operators comes from the capacity to reveal important personal information from the aggregation and analysis of small amounts of innocuous information. As a set of interconnected things silently sitting in the background of our lives, the IoT has the potential to produce extremely revealing virtual identities of people by gathering and connecting information from a

5 In this case, given the privacy implications Amazon sought to deny access to these request logs (Ferguson 2018). The defendant ended up allowing access to the request logs.

range of sources. Combine the information gathered from a Fitbit,[6] TV habits (Schiffer 2019), recorded conversations (Matyszczyk 2015), grocery purchases (Hill 2012), and sleeping habits (Bianchi 2015) and a highly revealing identity emerges of the person who is the source of information.

It is not just the ubiquity of the surveillance devices that makes the IoT an ideal surveillance network, but the fact that these things are informationally connected to each other, connections the users and consumers are likely to be unaware of. This means that people will be largely ignorant of the network of devices that have them under surveillance. Furthermore, people will be unaware of just how revealing the virtual identities produced by aggregation of information from the range of things in IoT can be.

As mentioned, the IoT differs from the internet in that the IoT exists in, and can be active upon, the physical world. While privacy concerns about the internet are not new at all, the fact that the IoT can infiltrate and integrate itself into every aspect of our lives means that the capacity of the IoT to gather information is vastly greater than the internet on its own. Second, the IoT presents a capacity to respond to the aggregated and analysed information in ways that the internet cannot. Consider if I was to make a request for a car sharing service, but it turns out that I am on a state watch list for anti-social behaviour, and thus any personal travel is constrained. As the IoT exists in the physical world and can directly control, constrain, and contort my behaviours, the potential power that can be exerted against me is both significant and subtle.

The power can be significant in that my life can be substantially disrupted. Consider an extreme example where surveillance of my private conversations suggests that I am a political dissident. Now, consider that I live in a smart house that has smart locks on the doors to the house.[7] Should the state have access to these smart locks it could effectively place me under house arrest. The IoT can also exhibit subtle power against me. Should I hear that my friends and colleagues have been locked down in their smart houses due to suspicious political activity, that would likely act as a significant chilling effect against me pursuing similarly dissident activity. 'Merely organizing movements of dissent becomes difficult when the government is watching everything the people

6 To show how revealing sports/activity devices like Fitbit are, in 2018 a university student was able to identify US bases for military and intelligence operations using an online source of information on Fitbit users (Bogle 2018).

7 A smart doorbell company, Ring, has partnered with 400 police forces in the US (Harwell 2019). This suggests that the integration of smart home technologies with domestic policing agencies is already occurring.

are doing' (Greenwald 2014, p. 177). Knowing that I may be watched by the state and knowing that the state can control my physical movements would already have a powerful effect chilling free political activity.

I have outlined aspects of the IoT that make it not just an ideal tool for surveillance but a potentially powerful tool for state control. Its ubiquity and capacity to remain unobserved in everyday life mean that the IoT can be engaged in surveillance of huge numbers of people. The increased power of information analytics mean that the information gathered from a myriad of connected IoT devices can be highly revealing, and the capacity of the IoT to act in the physical realm means that power can be exerted over people. In short, the IoT presents a surveillance network of unparalleled reach and power.

3 Personal Information and Privacies

One standard moral, legal, and political concept used to deal with surveillance and its impacts on people is privacy. That the IoT has great potential to violate people's privacy in a range of ways seems sensible and obvious, though it is open to a significant counter-claim. If, as described, the IoT can gather, process, and handle personal information without humans necessarily having any access to that information, has any privacy violation actually occurred? While this might seem counter-intuitive, consider a dog watching me in the shower.[8] Though we can understand why I might feel psychologically uneasy about the dog watching me, it just doesn't feel right to call this a violation of my privacy. IoT devices are similar; until a human accesses that information, while controversial, it is not immediately apparent if my privacy has been violated.

I want to suggest here that this is because of two interrelated points. First, we need to understand what sort of information we are talking about. I will suggest that there are two ways of thinking of information, as thin and as thick, and when thinking of privacy in an interpersonal sense, it is only as *thick information* that privacy becomes relevant. Second, there are two ways to conceptualise privacy. The first is based on interpersonal relations, the second between an institution like the state and its citizens.[9] As we will see, information

8 I thank Kevin Macnish for introducing me to the *dog watching me in the shower* example.

9 There are important relations between powerful institutions and people such as the relations between social media companies and their customers that are now of similar moral concern to that of the state and its citizens. However, the focus for this paper is on the state and citizens as the moral actors of concern.

handling systems like the IoT can be structured in ways that preserve the interpersonal conceptualisations of privacy, but that overstep the boundaries of legitimate state actions. The basic conceptual difference between the two ways of thinking about privacy turns on the recognition that interpersonal notions of privacy rely on information having semantic content, while the state–citizen notions of privacy rely on constraints to state power.

As stated in the introduction, I am taking a pluralistic approach to privacy. This builds on the recognition that privacy is conceptually messy. Inness (1992) opens her book *Privacy, Intimacy and Isolation* with the following:

> 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; it seems it will be a simple task to locate the conceptual and moral core of such an often-used term. But then the ground softens and we discover the confusion underlying our privacy intuitions. We find intense disagreement about both trivial and crucial issues. (p. 3)

There seem to be two general approaches to finding one's way out of this swamp, one – the unitary approach – where one offers a conceptualisation 'of privacy in the form of a unified conceptual core' (Koops et al. 2016, p. 487). The other – the pluralistic approach – 'offers typological or pluralist conceptions of privacy by making meaningful distinctions between different types of privacy' (Koops et al. 2016, p. 487). This second approach is taken here to suggest a distinction between two related but different conceptions of privacy. One is interpersonal; the other is political. I note that they are related, and that insofar as political relations can ultimately be reduced to interpersonal relations the political conception might be a subset of the personal. However, given the particular relations that arise between citizens and their governing bodies, if this is a subset of interpersonal relations, it is a particularly important one.

This pluralistic approach begins with the starting point that recognises there are a range of different privacy concepts and conceptions, and it is arguably an open question if there is any *right* account. However, this does not mean anything goes. In line with a pluralistic rather than relativistic approach, there is still a narrow and constrained set of ways with which we can meaningfully talk about privacy. This is a point recognised by Solove (2008), Nissenbaum (2009), Koops et al. (2016), amongst others. The reason for this pluralistic approach is that, as Solove (2008) has argued, each of the different positions offered by different thinkers through the years can be found to be too vague, too broad, or too narrow. As I have argued, these criticisms can be made against Solove's approach as well (2017a, p. 47 ff.). Drawing on legal theories that see property as a bundle of different rights, with some in play in some contexts, and others in play in other contexts, the pluralistic approach makes use of the different

concepts (Henschke 2017a, p. 47 f.). My aim here is to show that, despite the recognition that inhuman systems may not necessarily violate an individual's privacy when considered in an interpersonal context, we find reasons to understand and be concerned about inhuman systems when considered in a political context.

So why take a pluralist line, why not go for a unitary approach? The pluralistic approach makes it conceptually messy and may seem to suggest an 'anything goes' approach. However, as Koops et al. have shown, a multifaceted pluralistic approach can be clear and set useful conceptual boundaries. As Inness recognised, this description of the swamp of ideas is accurate. Underpinning the motivation to explain privacy with both interpersonal and political accounts is the recognition that inhuman systems can cause us to *feel* like privacy is violated, but this cannot be easily explained by interpersonal accounts of privacy.

> Closer examination demonstrates that these feelings are misplaced and that our language can be sloppy, and where there are genuine violations of privacy these are explained by the [political] account ... Nonetheless, while language does not always aim at moral exactitude and so we can see why what we say may not always mirror the truth, it is important to dig deeper to examine why it is we might feel as if a violation of privacy has occurred when in fact none has [on the interpersonal account]. (Macnish 2018, p. 423)[10]

The problem that inhuman systems expose is that interpersonal accounts of privacy cannot easily explain why we should be concerned about state use of inhuman systems. On the other hand, political accounts do not capture all the issues of privacy: the interpersonal accounts are still very important, valid, and useful. The point is not to jettison the interpersonal accounts. Instead, I seek to show that the interpersonal account cannot explain why inhuman systems are problematic, whereas the political account can.

Finally, one may wonder at the utility of keeping the term privacy at all. Van den Hoven's (1999, 2008) work uses the terminology of data protection instead. Part of the reason is that the term privacy has social resonance. As captured by

10 I note here that Kevin Macnish (2018) is making a different point, one about the distinction between access and control accounts of privacy. Moreover, that on his argument, the 'control account of privacy is mistaken' (p. 417). He therefore seems to be taking a unitary approach, which is in contrast to my pluralistic approach. However, following Koops et al., I consider that control and access are both forms of privacy (Koops et al. 2016). But I think Macnish's point is an important one: first, to recognise that the sense of privacy loss with inhuman systems is an important start to an analysis of whether a privacy violation has occurred. Second, that the language issue is secondary to the need to explore the ethical concerns that underpin the use of that language.

Samuel Warren and Louis Brandeis' seminal text *The Right to Privacy* (1890), there is a utility in keeping a singular linguistic reference. Furthermore, following Julie Cohen (2012), privacy cannot 'be reduced to a fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic' but is rather dynamic and 'shorthand for breathing room to engage in the process of boundary management that enable and constitute self-development' (2012, p. 1906). Privacy acts in a shorthand way to capture and express particular concerns about the relations between people, citizens, and the state. In, particular, when talking about political conceptions of privacy, privacy is, I believe, a useful term to express some significant concern about the way the state and its agents are relating to or interacting with its citizens.

3.1 Information: Thin, Thick, and Personal

To set this up, we first need to look at the concept of information and then see what is meant by 'personal information'. Picking up on Luciano Floridi's discussions of the philosophy of information (2002, 2004, 2005, 2011, 2019), I have argued elsewhere that we can conceptualise information in two ways: *thinly* and *thickly* (2017a, pp. 126 ff.). The thin account of information sees it simply as well-ordered data. That is, the data can be a string of letters, numbers, etc. that are ordered in a way that corresponds to some syntax.

> Consider the numbers 04092011. Depending on the rules of the system, presenting them as 11029040 or 04092011 can give different information ... it is not the order alone, but the recognition of the rules that govern the order that change the information. Think again of the numbers 04092011. If this is written as '04/09/2011' it may refer to a date. However, for an Australian these numbers correspond to the date 4th of September, 2011, while for an American, these numbers correspond to the date 9th of April, 2011 ... The data may remain constant but by changing the rules, the syntax, the information changes. (Henschke 2017a, p. 130)

This, however, is a deliberately thin account of information. We can also think of information in a *thicker* sense, as being meaningful, that is, having semantic content. Rather than just being well ordered data, this conceptualisation sees information as being well ordered data that is also *meaningful*.

> Think again that data 04/09/2011 can provide two different tokens of information. One refers to the 4th of September 2011, while the other refers to the 9th of April 2011. An explanation for the different information is that the conventional uses correspond to Australian and US meanings. When I communicate with Australians, because I am assuming the Australian day/month/year

> convention, I assume that they *mean* the 4th of September, 2011. When I communicate with Americans, because I am assuming the American month/day/ year convention, I assume that they *mean* the 9th of April, 2011. In this way, the assumed conventions point to an assumed meaning. (Henschke 2017a, p. 131, emphasis in original)[11]

Thus, we have information as thin or thick. As I will show, thick information is involved in interpersonal accounts of privacy, but not necessarily in political accounts of privacy.

To make the distinction clear, consider a digital photograph of someone. On the thin account, it is simply differently coloured pixels arranged in a particular form. Well-ordered data and nothing more. On the thick account, however, these well-ordered pixels might be a photograph of me meeting secretly with an enemy of the state. Now there are complex meanings associated with the ordered data. Moreover, these meanings vary depending on the person viewing the photograph. For an average person it could just be a photograph of two people meeting in a dark underground carpark. For someone in the intelligence service who knows me and knows the person I am meeting, this photograph could mean that a significant breach of national security is occurring. The point here is twofold. First, on the thick account of information, a set of ordered pixels carries with them a host of potential meanings. Second, on the thick account of information, the meanings vary with the observer.

As far as discussions of privacy are concerned, not all information is relevant. A data set about the moon's movements, whether thin or thick, hardly seems to have anything relevant to a discussion of privacy. Instead, I want to suggest here that privacy is concerned with *personal* information. By personal information I mean simply 'information that relates to a person or group of people in some way' (2017a, p. 268).[12] According to this approach, when an

---

11 This approach draws from Paul Grice's take on meaning as intention. The meaning of a given utterance, statement, written communication and so on is derived from the intention to which a speaker has for their utterance. For more on this see (Henschke 2017a, pp. 13 ff.; Grice 1957; Neale 1992).

12 In this context, we can understand personal information as relating to a person or group in two complementary ways. First, the person or group can be sources of personal information and, second, the person or group can be the targets of personal information. I make the distinction as follows: when a person is the source of personal information, they 'provide the initial Thin Information to the observer and from this Thin Information, [meaningful] information is formed and experienced as a [virtual] Identity' (2017a, p. 269). In contrast, a person or group is the target, 'where an observer has Semantic Information that targets a person or group of people. The more focused on a particular person or people, the narrower the target information is, and the more people captured by a given data set, the broader the target information is' (2017a, p. 268). If I am under surveillance, I am the source of personal information. If a group of

observer makes a connection between a data set and a person or group, the thin information has been made meaningful; it is now thick information. Finally, to be clear, not all personal information is private, though all private information is personal information.

3.2 Privacy as Interpersonal

To move now to discussions of privacy, consider that a photograph of me in the shower has been posted online, and I either didn't consent to it being taken or didn't consent to it being made public. In this case, we would typically say that a privacy violation has occurred. To unpack this claim, we need to clarify what we mean by privacy.[13] In a theoretical approach, for some, privacy is secrecy and that which is public is by definition no longer private (Solove 2008).[14] For others, privacy is a right by individuals to be let alone (Warren and Brandeis 1890). This can then be extended to conceptualise privacy as a space or boundary. Privacy 'is a set of boundaries we create between ourselves and others' (Solove 2008, p. 74). We might then think of privacy as control. 'Control-based definitions of privacy function by giving the individual control over a certain area of her own life, in other words, they give the individual *a specified realm of autonomy* ... we have every reason to embrace the idea that privacy provides people with *control over some area or areas of their lives*' (Inness 1992, p. 47, 53, my emphasis). These are descriptive accounts of privacy: they describe what privacy *is*.

In addition to theoretical approaches that say what privacy is, privacy has been conceptualised in relation to value, that is, why privacy matters. Jeffrey Reiman (1976) argues that privacy is a necessary component for self-development as it 'protects the individual's interest in becoming, being, and remaining a person' (p. 44). Expanding on this line, James Griffin (2008) holds that privacy typically is something necessary for us to develop as humans. 'Without privacy, autonomy is threatened ... It takes rare strength to swim against strong social

police officers decides that I am a criminal, then I am the target of personal information. A single person can be both the source of and the target of personal information.

13 Elsewhere, I have suggested that single reductionist approaches to privacy miss important aspects that our conceptions cover, and so argue that we should see privacy as a bundle of concepts (2017a, pp. 28 ff.). For an overview of the descriptive and ethical conceptions of privacy, see (Henschke 2017a, pp. 29–55). For sustained analysis, see (Inness 1992; Nissenbaum 2009; Solove 2008; Koops et al. 2016).

14 This notion of privacy as secrecy is described by Daniel Solove, but I note that he does not endorse the secrecy view (Solove 2008, pp. 21 ff., p. 111).

currents ... The richness of personal relations depends upon our emerging from our shells, but few of us would risk emerging without privacy' (p. 225 f.). Yet another approach takes privacy to be intimacy, relating to things that a person likes, loves, or cares about (Inness 1992). More recently, in the face of evolving information technologies, others have sought to define privacy in consequentialist terms (Solove 2008) or to reconceptualise it as 'context relevant information norms' (Nissenbaum 2004) or data protection (van den Hoven 2007).

For the purposes of this paper, I do not want to specify which conception is the best or stronger. Rather I want to point out that these approaches all have two things in common. First, these concepts understand privacy in the context of interpersonal relations. Second, they all rely on thick information. By interpersonal relations, I mean that the ways that privacy has been conceptualised draws on a foundation of interpersonal relations. The fundamental actors that frame the conceptualisations are people interacting with other people. They are semantic agents engaging with personal information in some way or another. Second, whether we consider privacy to be about secrets, information, control of information, intimacy, personal development, context relevant informational norms, or data protection, they all turn on the notion of thick information. In these conceptions, privacy relates to meaningful personal information that is being shared among people in some way. And the relevant factor is that this information is meaningful. If I was to have a stack of intimate photographs in a cabin in Antarctica, and the winds blew the cabin's doors open such that the intimate photographs were strewn all over the cabin, there would be no breach of my privacy. If, however, someone entered the cabin and started looking through the intimate photographs, we might then have a breach or violation of my privacy because another person is now accessing that thin information: they are making sense of it.

To make this directly relevant to the discussion of the IoT and state surveillance, most interpersonal accounts of privacy will only see a privacy violation occurring if the information being gathered, accessed, or communicated is meaningful. That is, people have to engage with the information in some way to make it a privacy relevant interaction. Contrast now the dog watching me in the shower versus a peeping Tom watching me in the shower. They both have access to the same thin information, but as the dog is not a semantic agent in the same way that a human is, it is only in the second case of the peeping Tom that my privacy is being violated. If it seems strange to talk about a dog violating my privacy, it is because we do not see animals as semantic agents in the same way that humans are. That is, they are not producing the semantic content for thin information in the same way that a human observer does.

The overall point then is that thick personal information, information made meaningful by being accessed by a semantic agent, is necessary for a working conception of privacy. Moreover, on many of the traditional accounts of privacy, the relevant factor is that the information is interpersonal: it has to be personal information, and it has to be observed, accessed, or experienced by another person. Thus, we have a cluster of privacy conceptions that draw on thick information and that are interpersonal. Contrasted with intimate information being strewn around by wind or a dog watching me in the shower, the interpersonal accounts of privacy all have meaningful information, thick information, at the core of their conceptualisation.

3.3 Privacy as Political

A different conception of privacy sees privacy as *political*. That is, rather than being centred on the notion of personal information and interpersonal relations, this conception of privacy frames the concept in relation to state–citizen relations. Rather than simply being between two people, the relevant relation in this conception is between the state and its citizens, or some variant thereof. And, rather than being about personal information *per se*, the relevant aspect is how that personal information plays a role in the use of state power against its citizens. In typical discussions, this political conception of privacy is about the use of, and over-extension of, state power against its citizens.

By describing privacy as political, this conception takes it that privacy is the realm where one specific actor, the 'state', cannot enter. In this explicitly political sense, privacy is seen as opposed to government intrusion:

> Private describes that zone that the government is not permitted to interfere in ... A person's home, for example, is private. And whatever happens there is none of the government's business – 'abnormal' sexual activity, drug use, religious or political gatherings. Insofar as they occur behind closed doors, they occur in a zone or space that is sheltered from government scrutiny. (Henschke 2017a, p. 39f.)

One way to capture the relevant difference between interpersonal conceptions of privacy and political ones is that the relevant actors are different. Now, rather than simply being about interpersonal relations between two moral agents, the relevant actors are now 'the state' and its citizens.

Consider again a smart house full of IoT enabled devices. While I might have purchased all these devices and feel happy with the various companies gathering, analysing, and using my personal information, I may become concerned if it turns out that the state is monitoring this information. Part of the reasoning is that privacy

is necessary for liberal democracies to function: 'it is either a necessity for liberal democracies or, without it, people's behaviours and their beliefs are "chilled" by the fear of government reprisals. On its necessity for democracy, proponents argue that 'the political role of privacy is not a matter of empirical contingency but has the status of a necessity' (Henschke 2017a, p. 40 f.). As Dorota Mokrosinska puts it, 'Moving beyond the arguments that present privacy as facilitating forms of political participation and increasing the effectiveness of the decision-making process ... privacy [is] constitutive of the liberal model of political legitimacy ... privacy is implicated in the idea of public justification that liberals place at the core of legitimate political order' (Mokrosinska 2014, p. 375).

Parallel to the necessity of privacy for political activity in liberal democratic states, is the fear that state surveillance will chill legitimate social activities and political expression.

> If we know or think that we are being watched, our behaviours will change ... [and] such changes can be detrimental to political freedom. If I know the government is likely to be watching me, then I am less likely to engage in behaviours that might be seen by the government as contrary to their interests ... In short, the idea of widespread government behaviour 'chills' free political behaviour and association. (Henschke 2017a, pp. 40f.)

The idea here is that liberal democracies not only allow for but ought to actively support their citizens' free beliefs, movements, and association. If those citizens have concerns that they are under surveillance, their beliefs, movements, and association will change. They may no longer feel free to express particular political ideas: they will not meet to discuss those beliefs and so on. The fear is that with widespread government surveillance, political cultures will change and those cultures that are at odds with the government's views will be driven underground. So privacy is necessary to safeguard political freedoms and to ensure that a nation's citizens are not behaving differently due to fear of state surveillance.

One of the important features of privacy-as-political conception is that, as per the social contract, the state has significantly greater power than I have as an individual: the state has a monopoly of violence. In Max Weber's (1920/2012) definition of the state, this monopoly of violence is a necessary feature of the state. The

> compulsory political association with continuous organization will be called a 'state' if and in so far as its administrative staff successfully upholds a claim to the *monopoly* of the *legitimate* use of physical force in the enforcement of its order ... The claim of the modern state to monopolize the use of force is as essential to it as its character of compulsory jurisdiction and of continuous organizatio. (p. 154, 165, original emphasis)

By definition, the state has power that I have ceded to it as a citizen. And while, as per the social contract, that power might be legitimate and used legitimately, outside of special circumstances,[15] the state must be constrained in how it operates. Privacy, the protection of a space from unjustified state intrusion, is an essential feature of liberal democratic states.

In the political conception, privacy is not about some peeping Tom watching me, but about the state encroaching on my personal space. In liberal democracies, entering my personal space is a violation: the state is overreaching. As per the social contract, as a citizen I give up certain rights in order for the state to provide me with security and other collective goods. But against this, the privacy-as-political conception ensures that I do not give too much away, that the state stays within its mandated areas and does not violate the social contract.

We can think of the political conception of privacy as a shorthand way of designating some area of interest or concern in which privacy is an instrumental term, but note that instrumental does not necessarily mean that the political conceptions of privacy are simply consequentialist. Privacy may be used to secure important rights, like a right to self-development. In particular, in the political account of privacy, privacy may instrumentally protect rights to self-development, free belief, and association. These all have particular importance for liberal democracies. Furthermore, I would say that any use of the term privacy is going to be instrumental. In any analysis of privacy, privacy is not considered valuable in and of itself, but because of the ways that it allows for, protects, and secures the privacy types identified by Koops et al. (2016): bodily privacy, spatial privacy, communicational privacy, proprietary privacy, intellectual privacy, decisional privacy, associational privacy, and behavioural privacy (p. 566 ff.).

As shown in Koops et al. (2016), we may be interested in many of the underpinning privacy types rather than in privacy itself. Following Koops et al., the interpersonal account might also show how and why the state should not invade my privacy, but I would suggest it misses some important aspects of the analysis. In particular, by using the political account, we are better able to understand specific politically important rights that are protected by privacy,

15 As per the social contract, the state can encroach on individual privacy in certain circumstances, however such circumstances must be special and special justifications need to be sought. A warrant to tap a citizen's phone is a process to ensure that such surveillance is necessary, proportionate and discriminatory.

and we are also better able to specify and perhaps quantify the rights violations and/or harms that can come from a government agent accessing, using, or distributing personal information.

The overall point here is that seeing privacy as political rather than interpersonal shifts the actors and changes the sets of things that need to be thought of when considering personal information. Any discussion of privacy as political should include considerations beyond those that are explicitly about personal information. Political discussions about free speech, the public communication of ideas, and the chilling effects of state surveillance on the free assembly of citizens and so forth are as essential to the discussion of privacy as issues of access to personal information. Moreover, in the privacy-as-political conception, special care needs to be taken with particular actors. Given the important role of the media in informing citizens about political realities and holding political leaders to account, journalists, for instance, may require special protections from state surveillance above and beyond those of the typical citizen. The privacy-as-political conception, then, would hold that journalists require stronger protections against government surveillance than the typical citizen does.

Furthermore, conceptualising privacy as political sees personal information as relevant but only insofar as it relates to the use of state power: The gathering and use of personal information needs to be understood as it relates to state power and its impacts on citizens. Whereas I may simply be offended if a peeping Tom were to watch me in the shower, if it were a state agent who had me under surveillance, I would be justifiably doubly concerned. It is not just that some human is invading my privacy. If they were doing this for some state-based reason, I would likely be worried about *why* the state wants to see me in the shower. Why are they doing this, what information do they want from me, how are they likely to use it against me, and what processes justified this intrusion? The concern here stems from the recognition that the state has power that it can wield against me, and as a single citizen, I am very limited in my ability to push back against such actions by the state. If a person taking control of my information is a member of the state 'then the consequences of my worrying that my information has been accessed, or will be accessed if I upset the state are severe. I may feel chilling effects that deter me from engaging in democratically legitimate but unpopular … demonstrations against the government' (Macnish 2018, p. 428). These concerns are about personal concerns like the right to self-development, as well as collective concerns, what Koops et al. (2016) call associational privacy, which is 'typified by individuals' interests in being free to choose who they want to interact with' (p. 568). Access to personal information is thus not just about the state accessing intimate and revealing

information about me, but also about what they will do with that information, what they want with it, and what I fear they will do with it.[16]

There are two possible concerns that I would like to address. Rather than seeking to understand privacy as both interpersonal and political, some might instead seek to combine both approaches by developing a unitary theory of privacy with 'a unified conceptual core' (Koops et al. 2016, p. 483). For instance, given that the focus in this paper is on information, perhaps we could unify both interpersonal and political accounts by seeing privacy as informational control. However, reducing privacy to informational control is problematic for three reasons. The first is that privacy, even informational privacy, can also be understood as access rather than control. For Kevin Macnish (2018), privacy is better understood as information access rather than information control. On his account, information control is still ethically, socially, and legally important, but it is not privacy. While I find much to agree with in Macnish's approach, I think there is no general agreement about whether privacy is information control or access. In line with the multifaceted pluralistic approach, I am inclined to suggest that it is both. The second is that privacy is not just informational. This is something that Koops et al.'s (2016) multifaceted typology details quite effectively. In their approach, there are eight primary ideal types of privacy, bodily privacy, spatial privacy, communicational privacy, proprietary privacy, intellectual privacy, decisional privacy, associational privacy, and behavioural privacy (p. 566 ff.). They then 'conceptualize informational privacy … as an overarching aspect of each underlying type, typified by the interest in preventing information about oneself to be collected and in controlling information about oneself that others have legitimate access to' (p. 568). In this approach, informational privacy is in Peter Blok's words 'the other side of the coin' (cited in Koops et al. 2016, p. 568). 'All (more or less) physical types of privacy lie on one side, and informational privacy on the other' (Koops et al. 2016, p. 554). The third is, perhaps given the focus of this paper on information in inhuman systems, that informational privacy is the correct layer of analysis to use. However, in line with the argument put forward here that we need to understand these inhuman

16 A related point here is that much more attention needs to be paid to the role of, and impacts of, powerful private companies on citizens. As we gradually gain an understanding of the capacities for social media to impact elections and political communities more generally, the power of these institutions is approaching that of the state – Shoshana Zuboff's (2019) discussion of *surveillance capitalism* is especially relevant here. I suggest here that we need an increasingly sophisticated discussion of the social licence granted to private companies that parallels that of the social contract. Such a discussion would focus on social licence rather than the social contract. Much more could be said about this issue. However, given the focus of this paper, my attention is on state surveillance issues.

systems in a political context, the agents change. We are no longer talking about information simpliciter, but information in a political context, specifically, the ways that information is used in and potentially disrupts the relations between a citizen and their state. Reducing privacy to information control would obscure this important relation.

Another concern with the political account is whether this is just a subset of the interpersonal. In some ways this is true, in that the political account is ultimately about people. Citizens are people, and the state is composed of people acting as agents of the state. However, I think that drawing attention to the political aspects of privacy is both descriptively and normatively important. It is a descriptively useful move as it can help explain why people feel that their privacy is at risk in an inhuman system, a feeling that cannot be explained by the interpersonal account. It is also a normatively useful move as the relations between citizens and the state are very significant relations, particularly in liberal democracies. Moreover, because of the power that the state has in relation to its citizens, the agency of the state is of particular moral, social, legal, and political importance. Reducing privacy to interpersonal accounts misses and obscures a range of important features that must play a role in our moral analysis of privacy.

The brief summary here is that privacy can be conceptualised in two distinct ways. In the first, a more traditional reading of privacy sees it as interpersonal. In the second, privacy is seen in political terms, about issues arising when the state encroaches on the spaces of its citizens, including informational spaces. One of the relevant differences between the two approaches turns, at least in part, on the actors. In the interpersonal conception, privacy is concerned with people as the primary moral actors, whereas in the political conception, privacy is concerned with the state and citizens as the relevant moral actors. A further difference is that in the interpersonal conception, privacy can be understood by reference to the production of and access to personal information that is thick, that has meaning due to the people accessing and handling that personal information. In the political conception, privacy includes personal information but must also include a recognition of the power relations between the state and citizens. As such, power relations are more relevant to the assessment of the situation than whether the information is thick or thin. A broader point is that it is a mistake to try to *simply* use the foundation of interpersonal conceptions of privacy for discussions of state surveillance. Again, while these interpersonal foundations are important, in particular the role that personal information plays, they do not capture additional important elements like power, free speech, chilling effects, political assembly and the like that are core to political conceptions of privacy.

4 The IoT and Privacies: Handling Personal Information in Inhuman Surveillance Systems

So, to bring the discussion, together recall that we have the IoT, an integrated network of things, which can be used to place us under surveillance and which has the potential to cause changes in the physical world. We also have the notions of thin and thick information. Finally, we have two conceptions of privacy, one as interpersonal and one as political. We are now in a better position to investigate if the IoT necessarily violates people's privacy when it gathers information on them. For this paper, I will suggest that the IoT does not necessarily violate privacy in the interpersonal sense, but that if the IoT is used by the state as part of a surveillance system, it does infringe on privacy in the political sense.[17]

To explain, let us return to the Amazon Echo. This scenario is set slightly in the future when Amazon's order fulfilment and shipping are conducted by robots and drones. I make a request through my Echo to purchase a pair of shoes. The purchase request is verified by my biometrics. The particular pair of shoes are located and taken from the shelves in the storage centre by a robot. The package is then placed by the robot into an autonomous (driverless) truck. The truck drives to a drone depot in my city. From there another robot removes the shoes from the truck and places the package onto a delivery drone. That drone then delivers the package to my home address.

Now, in this scenario, no humans have interacted with my request in any direct way. All information relevant for the order fulfilment is handled by non-semantic aspects of the IoT. That is, at no point does any information become thick information: it does not have any meaning attributed to it by any semantic agent. In this scenario, it does not matter if the purchase was something innocuous like shoes, or something more intimate like medicine or pornography or something of political relevance like a manual on how to conduct a revolution. The system as described is inhuman; at no point is interpersonal privacy violated. As, we have established, interpersonal privacy necessarily relies on thick information, it is therefore possible for the IoT to engage in a set of operations that do not violate my privacy.

That said, it is important to note that such a scenario does have considerable *potential* for interpersonal privacy to be violated. If a human operator was

17 As I will discuss later, such privacy infringements are not necessarily violations. As with other personal information, it is possible for the state to justifiably have particular citizens under surveillance as long as the appropriate processes have been conducted.

to access any of the relevant personal information and was not justified in doing so, then we would have a potential interpersonal privacy violation. In order for the IoT to be non-privacy violating, all relevant personal information must be handled by non-human aspects of the IoT. Furthermore, any personal information associated with my order must be permanently deleted after the order has been fulfilled. I have argued elsewhere that innocuous personal information can *potentially* violate privacy (2017a, p. 257 ff.), and so any such information warrants special care. Macnish (2018) makes a similar point that draws on the political account: In societies with pervasive state surveillance where 'the implication is that people's actions can be controlled to some degree through instilling in them a belief that their privacy has been compromised, or could be compromised at any time, irrespective of whether it in fact has been or even could be compromised' (p. 425). This applies even if the personal information is anonymised. In the view proposed in my *Ethics in an Age of Surveillance*, even anonymous personal information, if aggregated and analysed, requires properly informed consent. Thus, if information about my purchases are stored by Amazon and used in ways that contravene what I consented to, we have a violation of interpersonal privacy, even if the information has been anonymised.

Finally, there are many instances of the IoT violating interpersonal privacy in practice. Smart TVs that observe people in their homes are privacy violating (Matyszczyk 2015). Recently there has been criticism levelled at smart devices like the Google Home, as these systems have used human operators to monitor requests to see if the speech recognition programs are working properly or not (AAP 2019). Here, the IoT is part of an interpersonal privacy violation due to the handling of that personal information by people. The point here is that in order for a set of actions involving the IoT to preserve interpersonal privacy, personal information must not come into contact with people. However, it is possible for actions in the IoT to engage with personal information whilst preserving interpersonal privacy. Thus, the IoT does not *necessarily* violate people's interpersonal privacy.

In contrast, if we change the relevant actors and now think about the state and its citizens, thus shifting our conception of privacy to the political notion described above, we do have privacy violations. As we will see, such violations might potentially be justified, but key processes must be properly completed. Recall that in the political conception of privacy, it is not just about personal information, but also about how that personal information is gathered, accessed, and used by the state, and how such gathering, access, and use impacts the relation between the state and its citizens. First, and perhaps most obviously, if the state is using the IoT as part of a widespread surveillance system, then it has vast amounts of information on its citizens. Such information

can be powerful and when in the hands of the state further exacerbates the power that the state can wield over citizens individually and collectively. Given the monopoly of violence of the state, in such a surveillance scenario, the citizens are both sources of information and potential targets.

In these situations, even if the information gathered remains unaccessed by human agents of the state, thus remaining thin information, such a surveillance program could potentially have a significant chilling effect. That is, should such widespread state surveillance of citizens become public knowledge, it is likely to have a significant impact on citizens' behaviour. As the widespread criticism of state surveillance programs following the Edward Snowden revelations show, people are very uncomfortable if they are the sources of information for such state surveillance (Greenwald 2014, p. 170 ff.). Thus, in contrast to the interpersonal accounts of privacy, even if the information is still only being handled by inhuman aspects of the IoT, on the political accounts of privacy, the IoT violates privacy.

A second, important aspect is that the IoT is not just about information gathering, it includes the capacity for physical actualisation in the world. Consider again that, as per a set of AI analyses, a non-human set of processes have derived from my personal information that I am a political risk. As such, my physical movements through the city are constrained: I cannot order a ride-sharing service to areas of special government concern. My ability to access public transport is also automatically suspended as my smart card won't allow me through the turnstiles at the train station and it is not accepted on the bus. And, in an extreme move, my house is locked down, and I am effectively put under house arrest. In a slightly futuristic scenario, all of these events could occur without a human handling any personal information, as it is completely automated. Again, in the political conception of privacy, we have a set of significant privacy violations, even if no human had any contact with any information. This is a privacy violation regardless of the physical actualizations that occur because political privacy is so closely linked with political freedoms and rights and because of the political context in which the analytic processes by AI on private information are undertaken.

This example represents a gross exercise of state power against a citizen by means of the IoT. However, we don't need to resort to imagined scenarios to see how comprehensive surveillance and physical actualisation can be used by a state on its citizens. The Chinese social credit system involves a huge network of interlinked surveillance practices. Moreover, the social credit system finds expression in the physical world. If you have been engaged in socially undesirable activities such as jaywalking, you can be publicly shamed by having your name and photo published in public places (Cheng 2019). And should your

social credit fall below a mandated minimum, you may be banned from access to public transport (Kuo 2019). As before, such actualisation of state decisions can potentially occur without any individual human necessarily having access to your personal information. Moreover, the purpose of the social credit is to chill anti-social behaviours. The simple fact that the state has you under surveillance and will actively use those surveillance products against you is designed to encourage you to change your behaviour. Thus, again, even if no interpersonal privacy violations have occurred, this is a clear example of the state using IoT surveillance networks to intervene in personal behaviour.

A final point is that such expressions of state power against citizens are always unjustified. In functioning liberal democracies, for instance, if there is significant reason to suspect that a citizen is breaking significant laws, then police officers, as agents of the state, can seek warrants in order to gather, access, and use personal information as part of an investigation. In standard warranting processes, for the application to be successful, it must be demonstrated that the request is necessary, that there is no other option than surveillance, that it is proportionate, that the potential illegal activity is serious, that the activity is serious enough to outweigh the right to privacy (Michaelsen 2010),[18] that it is discriminatory, and finally that there is sufficient intelligence or reason to believe that the specific person being targeted for surveillance is indeed involved in the illegal activity. The point here is that there may be situations in which use of the IoT by the state against particular citizens can be justified. However, such conditions need comprehensive and just oversight processes. Moreover, in liberal democratic polities, the target of such surveillance has a presumed right to privacy, and it is only in exceptional circumstances that any diminutions of privacy would be justified.

In short, what I have shown here is the threat posed by the IoT to people's privacy. Importantly, given the need to see information as thin or thick, I have argued that the IoT does not necessarily violate people's interpersonal privacy, as the information only becomes thick when handled by people. In contrast, however, I have offered a set of reasons why inhuman systems do violate people's privacy when used by states against their citizens. By seeing privacy as two conceptions, interpersonal and political, we are better able to understand and design our technological and legal infrastructures in ways that ensure that a core concept like privacy is effectively respected.

18 I note here such proportionality calculations are complex and often highly subjective, see Henschke (2018).

Acknowledgements: I thank CJ O'Connor for useful feedback on this paper, Kevin Macnish for insightful discussions on the nature of privacy, and the anonymous reviewers and editor for their useful feedback, comments, and suggestions.

Research for this paper was supported by funding from the Australia Research Council for DP180103439, 'Intelligence and National Security: Ethics, Efficacy and Accountability' and the European Research Council grant on 'Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies.'

Funding: This work was supported by European Research Council, Funder Id:, Grant Number: Project Title: Global Terrorism and Collective Mor, Australian Research Council, Funder Id: http://dx.doi.org/10.13039/501100000923, Grant Number: DP180103439: Intelligence And National Security: E.

References

AAP (2019). 'Google Listens to User Speaker Recordings', *SBS News*, July 11.

Allenby, B. (2013). 'Emerging Technologies and Just War Theory', in F. Allhoff, N.G. Evans and A. Henschke (eds.). *Routledge Handbook of Ethics and War: Just War in the Twenty-First Century* (Abingdon: Routledge), pp. 289–300.

Allhoff, F. (2011). 'What Are Applied Ethics?' *Science And Engineering Ethics* 17 (1): 19.

Allhoff, F. and Henschke, A. (2018). 'The Internet of Things: Foundational Ethical Issues', *Internet Of Things* 1-2: 55–66. doi: https://doi.org/10.1016/j.iot.2018.08.005.

Bianchi, M.T. (2015). 'Consumer Sleep Apps: When It Comes to the Big Picture, It's All about the Frame', *Journal Of Clinical Sleep Medicine* 11 (7): 695–696.

Bogle, A. (2018). 'Strava Has Published Details about Secret Military Bases, and an Australian Was the First to Know', *ABC News*, 30 January.

Cheng, K. (2019). 'Police in Chinese City Punish Jaywalkers by Classifying Them as "Untrustworthy People" in Country's Social Credit System', *Daily Mail*, July 9.

Cohen, J.E. (2012). 'What Privacy Is For', *Harvard Law Review* 126: 1904.

Connor, K. (2019a). 'Schedule an Uber or Lyft with Your Amazon Echo. Here's How.' *C|net*, June 24.

Connor, K. (2019b). 'Skip the Swiping and Ask Amazon Echo to Order Your Pizza for You', *C|net*, June 17.

D'Onfro, J. (2019). 'Amazon's New Delivery Drone Will Start Shipping Packages "In a Matter of Months"', *Forbes*, June 5.

Ferguson, A.G. (2018). 'Alexa, What Is Probable Cause?' *Slate*, November 20.

Floridi, L. (2002). 'What Is the Philosophy of Information?' *Metaphilosophy* 33 (1&2): 123–145.

Floridi, L. (2004). 'Information', in F. Luciano (ed.). *The Blackwell Guide to the Philosophy of Computing and Information* (Oxford: Blackwell Publishing), pp. 40–62.

Floridi, L. (2005). 'Is Semantic Information Meaningful Data?' *Philosophy and Phenomenological Research* 70 (2): 351–370. doi: 10.1111/j.1933-1592.2005.tb00531.x.
Floridi, L. (2011). *The Philosophy Of Information* (Oxford: Oxford University Press).
Floridi, L. (2019). 'Semantic Conceptions of Information', in E.N. Zalta (ed.). *The Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/archives/win2019/entries/information-semantic/>.
Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books).
Grice, H.P. (1957). 'Meaning', *The Philosophical Review* 66 (3): 377–388.
Griffin, J. (2008). *On Human Rights* Oxford: Oxford University Press.
Harwell, D. (2019). 'Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns', *Washington Post*, August 29.
Hearn, L. (2010). 'Google on Privacy: Change Your Name', *Sydney Morning Herald*, August 17.
Henschke, A. (2017a). *Ethics in an Age of Surveillance: Virtual Identities and Personal Information* (New York: Cambridge University Press).
Henschke, A. (2017b). 'The Internet of Things and Dual Layers of Ethical Concern', in P. Lin, K. Abney and R. Jenkins (eds.). *Robot Ethics* (Oxford: Oxford University Press), pp. 55–66.
Henschke, A. (2018). 'Conceptualising Proportionality and Its Relation to Metadata', in D. Baldino and R. Crawley. *Intelligence and the Function of Government* (Melbourne: Melbourne University Press), pp. 221–242.
Hill, K. (2012). 'How Target Figured Out a Teen Girl Was Pregnant before Her Father Did', *Forbes*, February 16.
Inness, J.C. (1992). *Privacy, Intimacy, and Isolation* (New York: Oxford University Press).
Knaus, C. (2018). 'Just 53 Australians Used Facebook App Responsible For Cambridge Analytica Breach', *The Guardian*, April 10.
Koops, B.-J., Newell, B.C., Timan, T., Skorvanek, I., Chokrevski, T., and Galic, M. (2016). 'A Typology Of Privacy', *University of Pennsylvania Journal of International Law* 38 (2): 483.
Kuo, L. (2019). 'China Bans 23m from Buying Travel Tickets as Part of "Social Credit" System', *The Guardian*, March 2.
Lewis, P. (2018). 'Trump Adviser John Bolton Worked with Cambridge Analytica on YouTube Voter Experiment', *The Guardian*, March 23.
Li, S., Xu, L.D., and Zhao, S. (2015). 'The Internet of Things: A Survey', *Information Systems Frontiers* 17 (2): 243–259. doi: 10.1007/s10796-014-9492-7.
Macnish, K. (2018). 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World', *Journal Of Applied Philosophy* 35 (2): 417–432.
Marshall, A. (2019. 'A Bet on Uber Is A Bet on Self Driving', *Wired*, October 5.
Matyszczyk, C. (2015). 'Samsung's Warning: Our Smart TVs Record Your Living Room Chatter', *CNet*, February 8.
Michaelsen, C. (2010). 'The Proportionality Principle, Counterterrorism and Human Rights: A German-Australian Comparison', *City University Of Hong Kong Law Review* 21 (1): 19–43.
Mokrosinska, D. (2014). 'Privacy and the Integrity of Liberal Politics: The Case of Governmental Internet Searches', *Journal Of Social Philosophy* 45 (3): 369–389. doi: 10.1111/josp.12068.
Neale, S. (1992). 'Paul Grice and the Philosophy of Language', *Linguistics And Philosophy* 15 (5): 509–559.
Nissenbaum, H. (2004). 'Privacy as Contextual Integrity', *Washington Law Review* 79 (1): 119–158.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press).

Reiman, J.H. (1976). 'Privacy, Intimacy, and Personhood', *Philosophy and Public Affairs* 6 (1): 26–44.

Schiffer, Z. (2019). 'Smart TVs are Data-Collecting Machines, New Study Shows', *The Verge*, October 11.

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

Solove, D. (2008). *Understanding Privacy* (Harvard: Harvard University Press).

van den Hoven, J. (1999). 'Privacy and the Varieties of Informational Wrongdoing', *Australian Journal of Professional and Applied Ethics* 1: 30–43.

van den Hoven, J. (2007). 'Privacy and the Varieties of Informational Wrongdoing', in J. Weckert (ed.). *Computer Ethics* (Aldershot: Ashgate Publishing), pp. 317–330.

van den Hoven, J. (2008). 'Information Technology, Privacy and the Protection of Personal Data', in J. van den Hoven and J. Weckert (eds.). *Information Technology and Moral Philosophy* (Cambridge: Cambridge University Press), pp. 301–321.

Warren, S.D. and Brandeis, L.D. (1890). 'The Right to Privacy', *Harvard Law Review* 4 (5): 193–220.

Weber, M. (1920/2012). *The Theory of Social and Economic Organization* (Eastford: Martino Fine Books).

Whitney, L. (2019). 'How to Shop on Amazon with Alexa Voice Shopping', *PC Mag*, 4 June.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs).