DATA, PRIVACY AND THE INDIVIDUAL

INTRODUCTION TO PRIVACY

KEVIN MACNISH
UNIVERSITY OF TWENTE

NOVEMBER 2019

INTRODUCTION TO PRIVACY

Dr. Kevin Macnish

University of Twente

Reference to this paper should be made as follows:
Macnish, K. (2019) "*Introduction to Privacy*".

INTRODUCTION

This paper forms an introduction to philosophical and legal thinking regarding privacy. It opens with an historical overview of privacy before proceeding to consider the meaning of privacy and whether there is a right to privacy. Finally, the paper closes with a look at two popular but flawed arguments regarding privacy. Throughout the paper I will draw on historical and contemporary issues in privacy to illustrate and highlight ethical concerns.

HISTORICAL OVERVIEW

To gain a full understanding of how privacy is viewed today, and why it is viewed as it is, it is helpful to get an historical overview of developments in legal and philosophical thinking regarding privacy. While privacy has been a central issue to most societies throughout history (Locke, 2010), it was not until 1890 that the first academic article attempting to define privacy was published. This article, 'The Right to Privacy' by US judges Samuel Warren and Louis Brandeis, was written in response to increasingly intrusive means (in their case, long-range camera lenses) of monitoring private gatherings of public officials and claimed that privacy was an instance of the general right 'to be let alone' (Warren and Brandeis, 1890). Following this article, definitions and applications of privacy were largely limited to the legal sphere, and particularly to US Supreme Court judgements. Of particular note are Olmstead vs United States (1928) in which the Court ruled that police tapping a private phone was not a violation of privacy. The decision was overturned in 1967 when a later Court ruled that police tapping a public (and by extension also a private) telephone was indeed a violation of privacy in the case of Katz vs United States (1967). More recently, technological developments have led to new privacy rulings concerning the use of tracking technologies attached to vehicles (United States v. Jones, 2012) and access to mobile phone information (Carpenter v. United States, 2018). After the Olmstead ruling, most US Supreme Court rulings have limited the ability of the state to interfere in private lives of citizens.

The rulings of the US Supreme Court are relevant to the broader, global debate on privacy given that most of the writers on concepts and theories of privacy have tended to be American. They are also relevant given that many of the judgements arose from challenges to privacy deriving from new technologies which were applied on a wider scale in the US before other countries. However, the European Parliament has made progress in this direction since the introduction of the Data Protection Directive in 1995 (EU Parliament, 1995; Lord, 2018; see below) while in China and across many African states there are remarkably few privacy protections in place.

Philosophical debates surrounding privacy are generally seen to have started with Judith Jarvis Thomson's paper on 'The Right to Privacy' (Thomson, 1975), which appeared in

Philosophy and Public Affairs. The same issue also published Thomas Scanlon's response to Thomson and James Rachels' paper on the value of privacy (Rachels, 1975; Scanlon, 1975). As a result, this issue set the terms of the debate for decades to come. In her paper, Thomson challenged the suggestion that there was such a thing as a right to privacy, arguing that privacy could instead be understood as a bundle of other rights. Scanlon disagreed with Thomson arguing instead that privacy was a matter of zoning, such that as matters came closer to a person (i.e. in public, moving to the home, moving to the individual) so they tended to become more private. Rachels' contribution was to identify the value of privacy as being a means to define relationships such that more intimate relationships tend to involve fewer boundaries around private details; I share more private information about myself with my wife than I do with my boss.

A separate discussion was started nearly ten years earlier by Alan Westin when he argued that privacy was a matter of information (Westin, 1967). While limiting privacy to information has potency in the data-driven world in which we live today, others such as Tony Doyle have responded that there are other aspects of privacy which are not information-dependent (Doyle, 2009). Doyle gives an example here of a pornographic actor whose naked body is available for all to see on film but who can still experience an invasion of privacy if a peeping Tom watches her undress. In the same paper, Doyle questions whether privacy has any inherent value, suggesting that if a normally private act is witnessed in such a way that there can be absolutely no repercussions, then nothing wrong has happened. The precise value of privacy has also been questioned by feminist philosophers who have pointed out that women have traditionally been confined to private spaces, and that a cover of privacy may prevent successful intervention by the state to protect women and children from domestic abuse and rape (Allen, 1988; Lever, 2005).

A further debate in the philosophical literature has centred on whether privacy is a matter of access to things deemed private, such as the naked body or a diary, or of controlling that access. The control account would hold that a person being in possession of my diary without my consent would be violating my privacy, whereas the access account holds that it would only be when the diary was read that privacy would be violated. In this debate, Julie Inness and Alan Moore have given the most spirited defence of the control account of privacy (Inness, 1996; Moore, 2008, 2003) while Anita Allen is the leading proponent for the access account (Allen, 1999, 1998, 1988). As Kevin Macnish has pointed out, where one falls in this debate will ground one's response to cases such as the Snowden revelations of 2013, which indicated that the National Security Agency had intercepted but not necessarily read the emails of potentially millions of people (Macnish, 2018). Legal scholar Daniel Solove, in identifying 16 different uses of privacy, has responded to the general lack of agreement on privacy issues by suggesting that we take a Wittgensteinian approach of recognizing a family of values that are encompassed by the

concept of privacy, albeit that the concept itself can never be clearly defined (Solove, 2008, 2006, 2002).

While debates on the meaning and extent of privacy continue, one of the most popular accounts in recent years has been that of Helen Nissenbaum (2009). Nissenbaum draws on Michael Walzer's notion of spheres of justice (Walzer, 1984) to suggest that privacy is appropriate to different contexts. Hence what is private between a patient and a doctor is distinct from what is private between a client and a lawyer. However, were the lawyer and the doctor to confer by sharing this information, there would be a breach of the appropriate contexts for the patient/client's privacy.

As in the US, so European laws have been prompted by technological developments, and particularly the internet. In 1995 the European Parliament introduced the Data Protection Directive (Directive 95/46/EC, 1995), which established seven principles related to data collection: giving due notice to the person whose data is collected, restricting purpose to that given for data collection, requiring consent, offering appropriate security, disclosing when data was collected, giving individuals access to data concerning them on request, and the ability to hold data collectors accountable. However, the Directive was non-binding and data privacy laws varied across Europe (Lord, 2018). Recognizing these limitations, and in response to the pervasive nature of the internet and increasing concerns regarding data collection, the European Parliament revoked the Directive with the General Data Protection Regulation ((EU) 2016/679, 2016), which came into force in May 2018. The GDPR, as it is known, has introduced stricter standardisation across Europe, requiring express permission from individuals in order to hold data relating to them, and giving people the so-called 'right to be forgotten.' This last enables individuals to have data relating to them removed from public access should they wish, provided it is not in the public interest for it to remain accessible (e.g. criminal convictions). The GDPR expressly concerns itself with personal data, which it defines as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (Art. 4 EU Parliament, 2016).

In summary, the last 130 years, and particularly the last 50 years, have seen a large amount of activity regarding privacy. Legal decisions have frequently been occasioned by developments in technology that have given the state and other actors (such as companies) access to hitherto private information, and have typically responded by restricting this access. Philosophical debate has tended to focus on the meaning, extent, and value of privacy.

WHAT IS PRIVACY?

As noted above, the exact definition and limits of privacy are highly disputed. In this section we will look in greater depth at some of the arguments raised above to get a clearer idea of the alternative positions. In particular, we will look at the debate concerning privacy as access or control, whether privacy is about information only, and why privacy should be valued.

We have seen that philosophers such as Julie Inness and Adam Moore hold that privacy is a matter of control. If I can control information about myself then I can consider that information private. Hence when the US National Security Agency collects my email, whether it is read or not, I have lost control of that email and so experienced a diminution of my privacy. Such surreptitious data collection may be justified if I am planning an act of terrorism against the US, but if I am not, and not suspected of such, then this diminution of my control over data about me is wrong and my right to privacy has been violated.

The privacy as control account is challenged by Anita Allen and Kevin Macnish, among others. Macnish has argued that a diary may fall out of the diarist's control but the diarist plausibly does not experience a meaningful loss of privacy (beyond the knowledge that he keeps a diary) unless the diary is actually opened and read. There may be a subjective and grounded fear of a loss of privacy, but just as a subjective and grounded fear of being attacked in the street is different from actually being so attacked, it is similarly the case that a fear of a loss of privacy is not sufficient for there to have been an actual loss (Macnish, 2018). It is plausible that there is a misunderstanding stemming from different interpretations of the use of control in the control account, but if so then descriptions of precisely what is meant by control are not easily come by.

A second area of contention noted above was that of whether privacy is a matter purely of information or whether it pertains to other areas as well. In a data-driven age, the correlation between privacy and information is easily seen, but as Doyle's argument concerning the pornographic actor given above demonstrates, there may be privacy violations which are not information-bearing. A similar example can be devised whereby the peeping Tom returns to look in through the actor's bedroom window night after night. Imagining the actor maintains a strict night time regime, after a few nights the voyeur becomes aware of this but continues to watch. For each successive night the voyeur gains marginal information (the routine is still being followed, there are no changes to the room) but we would still feel that a gross violation of the actor's privacy occurs each night.

Another non-information example of a privacy violation occurs in relation to space. Each of us has some notion of private space into which another may not intrude. Granted, just as with other aspects of privacy, the extent of this space will depend on the person and culture in which they are situated, but nonetheless there is a notion of private space at work here. I may have a conversation with a friend at a party which is not itself private,

but if we notice a third person listening to us, we might well feel aggrieved and decide to conclude the conversation elsewhere. The importance of personal space has significant implications for tracking people's movements through monitoring mobile phone use or wearable tracking technologies.

The extension of privacy has gone further to some writing about decisional privacy, the right for one's decisions to remain private, and republican privacy, drawing on Philip Pettit's approach to neo-Republicanism to argue that privacy is an essential pre-requisite for a functioning democratic system characterised by non-domination (Pettit, 2014, 2001). That is, a good democratic state is one in which citizens do not 'live under the arbitrary will or domination of others, … [the state promotes] the freedom of its citizens without itself coming to dominate them, … [and good citizenship involves] preserving the state in its distinctive role as an undominating protector against domination' (Lovett and Pettit, 2009). For a system to be undominating, it is necessary for voting to remain private to the individual voter, as well as to foster environments of safety whereby people can engage in democratic activities such as protesting without fear of reprisals (Regan, 1986; Solove, 2002).

These extensions take us to the question as to why privacy is valued so highly. After all, privacy appears to be a culturally-related phenomenon, as we have seen Nissenbaum argues (Nissenbaum, 2009). While it is true that what we consider private has changed with generations and is experienced differently around the world (just think of the relative social acceptability of the bikini in contemporary Europe as against Victorian England or modern-day Iran), the fact remains that every society studied appears to hold privacy as a value, even if it gets expressed or experienced in different ways (Locke, 2010).

In the light of Tony Doyle's argument about the 'perfect voyeur' referenced above, some might question whether privacy holds any value (Doyle, 2009). Doyle's argument holds that an alien at 100 light years away from Earth has complete access to your life and thoughts, but by the time the information reaches the alien, you will be dead. By the time any actions taken by the alien then reach Earth, your children and probably grandchildren will also have died, so repercussions will not fall on anyone with living memory of you. Doyle's point is that privacy only holds value while it can protect a person (or those with living memory of that person) from harm. Privacy is therefore instrumentally and not intrinsically valuable.

Whatever one's response to Doyle's argument, privacy does serve to protect a range of interests. At a very basic level, my privacy provides me with a sense of security: that you can't access certain information about me that I might find embarrassing or which could damage my reputation. In this way, I can experience autonomy, which itself can be both intrinsically and instrumentally valuable (Kant, 1969; Mill, 2006), with my thoughts and with trusted friends, safe in the knowledge that my private utterances or activities will not come back to haunt me. For example, I may enjoy an alcoholic drink on holiday and

share a picture with friends online which, if it came to the attention of my boss, could cost me my job (Moriarty, 2011). My autonomy might also be affected simply by your respecting my decision to keep my thoughts, my body, or other aspects of my life private, no matter how interested you may be in these aspects (Benn, 1971).

Through privacy I can also experiment with relative safety. I could probe political ideas that may be at odds with my peer group, or explore my sexuality, or experiment in other areas that may be proscribed by the society in which I live. Were these experiments in living to become widely known I might be crushingly embarrassed to the point of taking my own life, or put my life at risk with the state or my community should they take against my decisions (consider communities that persecute people for conversions of faith or homosexuality). Were my eccentricities to become known to a small number of people, I may be subject to social harms such as blackmail. In both cases, their remaining private gives me security and enables a degree of diversity within society—something which is generally perceived to be of value, particularly in democracies. Finally, my privacy can protect my dignity. There is no secret as to what happens when I use a public toilet, but it would be deeply humiliating were I forced to use the toilet in public with no door on the cubicle. The same can be said for having sex or getting undressed. Each of these is a potentially embarrassing activity for which we afford each other privacy out of courtesy and civility.

The value of privacy does not stop with the individual, though. We have seen already that privacy has an impact on Republican theories of the state in terms of providing a society which is non-coercive and encouraging of diversity. Even if we reject Pettit's notion of republicanism, the benefits for democracy of a secret vote are widely recognized (Lever, 2007). Were the government, or our peers, able to access our votes and associate them with us then we might vote very differently. Similarly, we might experience such chilling effects when considering engaging in democratically legitimate activities such as protesting. If I do not join a protest for fear of reprisals by the state then the state will not know the true extent of public dissatisfaction with its policies and an important means of holding the state accountable will have been removed as an option. Thus democracies become impoverished when privacy is diminished (Regan, 2002, 1986; Solove, 2002).

At the same time, such chilling effects can also be caused by companies, as well as communities or the state. While the state can imprison or in some cases execute a person, a company can fire that individual or treat them as a pariah if they act in a way that may be perceived to harm the company. This has often been the experience of whistleblowers such as Earnest Fitzgerald, who was demoted and then made redundant by the USAF after revealing overspend on the Galaxy aircraft in the late 1960s (Fitzgerald, 1972). Companies as well as the state can use surveillance to intrude on the privacy of individual employees of whom the company suspects of some action deemed inappropriate.

Furthermore, corporate invasions of privacy have expanded significantly in the last 15 years with the advent of social media data. Not only do companies surveil their employees, but also their customers. On one level his has allowed companies to engage with customers in a wholly novel manner, offering them more personalised services. On another level, though, it has provided some companies with an unprecedented insight into the lives of those customers, sometimes without their knowledge or consent. In the case of the recent Cambridge Analytica scandal, such intrusions have led to attempts to manipulate the political process through targeted, discrete advertising based on known but often private interests (Cadwalladr and Graham-Harrison, 2018; Tobitt, 2018).

There are two standard challenges in response to concerns about corporate surveillance. One is that the hardware and software used by employees and customers may belong to the corporation, so it is reasonable for the corporation to access them to ensure they are not being misused. The second is that access is needed for the smooth running of the network, and particularly for purposes of cybersecurity, which often requires profiling 'typical' employee and customer behaviour in order to identify atypical behaviour, which may indicate the presence of a hacker.

In response to these challenges, it should be noted that while a landlord might own a property, he does not have free range over that property while a tenant occupies it. The tenant is still entitled to her privacy, as is the employee on company machinery or the customer using corporate software or hardware. It is possible for the corporation to act against abuse of company property without monitoring every keystroke of every employee, which gives potential access to bank accounts or private emails. The concern regarding the network, and particularly cybersecurity, is a stronger argument. Even here, though, it is possible to develop profiles of typical employees without monitoring keystrokes or following web-browsing beyond the domain name server level (i.e. www.name.com/ but not www.name.com/sub-level). More challenging still is the use of "shadow profiles", profiles of non-users developed by social media sites such as Facebook (Hill, 2017). Originally these were created to connect people more effectively if and when they became members of the site, but have more recently been justified as a security measure (Brandom, 2018). While it may be reasonable to develop a profile of a typical user, built from information gained from consenting employees, it is far less so to develop the profile of a typical attacker (or, indeed user) built from information gained from non-consenting parties who have not even visited the site.

These reflections should give us pause for thought when we hear phrases such as 'privacy is dead' (Dhawan, 2009). The value of privacy, both to individuals and society, is clear. In its absence, our lives become less secure and society less democratic. As such, when privacy appears to be under threat by technology, it is essential that public debate occurs to weigh up the value of the technology relative to the risks to privacy. We have seen that this has arisen in US law with the development of long-distance camera lenses, the telephone, GPS tracking devices, and the mobile phone. In the wake of the leaks by

Edward Snowden, the extent to which privacy on the internet has been compromised by intelligence agencies has also come into the spotlight. More recently still, the aforementioned Cambridge Analytica scandal has demonstrated that it is not just intelligence agencies that can compromise privacy on the internet but social media and data collection companies as well (Cadwalladr and Graham-Harrison, 2018).

IS THERE A RIGHT TO PRIVACY?

Given the value of privacy both to the individual and society, do we have a right to privacy? Privacy is recognized as a human right in both the Universal Declaration of Human Rights (United Nations, 1948) and in the European Convention on Human Rights (Grabenwarter, 2014). Furthermore, we have seen that privacy is in the interests of the individual and society and an expression of autonomy on the part of both. These all add up to a strong case for recognizing privacy as a basic right. (For more on autonomy and privacy, see Karina Vold and Jess Whittlestone's paper for this project).

That said, it would be strange to see privacy as an absolute right. If so then murderers would have an argument against the state wiretapping their phones or reading their email. There needs to be a balance struck between the legitimate private interests of the individual and groups in society and the legitimate state interests of protecting the public from harm. Neither the Universal Declaration nor the European Convention present privacy as an absolute right, but as one that is tempered by national and security interests.

This nuance leads to the question as to when it is legitimate to diminish the privacy of another. The ethics of surveillance tends to revolve around lists of considerations that should be taken into account when considering whether an act of surveillance is legitimate (Allen, 2008; Lyon, 2001; Macnish, 2017, 2014; Marx, 1998). Most agree that there is a need for a legitimate cause, and that the act of surveillance should be proportionate to the incident occasioning the surveillance, but beyond that there is considerable dispute (Hosein, 2014; Macnish, 2014; Marx, 2014; Palm, 2014; Stoddart, 2014).

If privacy is a right, albeit one that is not absolute, to what extent can the individual waive that right? That is, is the right to privacy inalienable? This is a relatively recent consideration that has only received limited attention (Moore, 2015). Certainly some individuals do waive their right to privacy, such as those who expose themselves in public or contestants in some reality TV shows such as Big Brother. However, the fact that some people do waive their privacy rights does not mean that they should be able to do so. Adam Moore worries that attempts to prevent people from doing so would be strongly paternalistic, but even with that concern in mind there are further considerations regarding the protection that some groups might enjoy as a result of everyone respecting not only others' but also their own privacy. For example, if everyone who was

heterosexual declared themselves such, those remaining would, by inference, not be heterosexual. This could put the latter group at some risk in certain societies (Allen, 2011, 1998; Lever, 2013; Moore, 2013). This being the case it may follow that some aspects of privacy are inalienable, but it would be bizarre for every aspect of privacy to be seen as inalienable, for this would mean that we would never be able to share a private thought.

If privacy, or at least aspects of it, can be waived then this raises the importance of consent (for more on consent, see Kevin Macnish's paper on consent). With a person's consent, far more privacy can be diminished without necessary harm. If, for instance, I choose to publish my autobiography, then I will almost certainly experience a diminution of my privacy, but not in a manner that is problematic. I may unwittingly put myself at risk of exploitation or coercion, but the reduction of privacy in and of itself would be ethically acceptable (Macnish, 2017). By contrast, were you to publish a biography of me without my permission and drawing on documents that you had no permission to see, then the damage to my privacy would be significant.

Similar problems may be experienced in the corporate world with the so-called 'privacy paradox.' The paradox involves people claiming that they highly value privacy but then providing reams of personal data about themselves online for little or no recompense. If a person readily consents to parting with private data, then it is hard for them to complain if the recipient then uses that data. At the same time, data may be harvested by companies using loyalty cards (Duhigg, 2012) on the basis of minimal consent agreements (a tick in a box or a signed piece of paper with full terms and conditions only available online via a lengthy URL). In such cases, it is harder to claim that privacy has been consensually waived.

POPULAR ARGUMENTS

Aside from the academic arguments considered in this paper, there are at least two popular arguments that are frequently employed in discussions on privacy. The first of these sees privacy as the polar opposite of security, such that there is a zero sum game in attempting either to protect privacy or to guarantee security, and it deems security to be more important than privacy. The second suggests that, 'if you have done nothing wrong then you have nothing to fear' from a diminishing of your privacy. We will consider these in turn for the remainder of this paper.

The first of these arguments, setting privacy against security, draws from an understanding of the state's pursuit of national or societal security through monitoring its citizens. The aforementioned Snowden leaks demonstrate an example of this when arguing that the National Security Agency collected domestic call records (metadata) of US citizens' mobile phone use. Such data collection is necessary, the argument holds, in

order to secure the public from acts of terrorism; some privacy needs to be forgone for the greater good of society.

When cashed out in this way an equivocation in the argument becomes more obvious. It is not a matter of setting my privacy against my security, or the privacy of society against the security of society, but rather of setting my privacy against the security of society. While it would be unacceptable to have a few free riders gaining the benefits of security without paying needed costs, the argument is not so simple. Some further considerations are in order.

In the first place, when I am balancing up my privacy against my security, the two are not counter-poised. I value my privacy, as we have seen, partly because it gives me some security. If you remove (some of) my privacy then I will feel, and possibly be, less secure. The same is true when the whole of society loses a degree of privacy to gain a degree of security. Hence the misconception in the argument is that the privacy right of an individual can be weighed up against the security rights of the group, in which case the individual is likely to lose. However, as demonstrated here, privacy and security cannot be separated so easily.

In the second place, it is rarely the case that all of society loses the same degree of privacy to gain the same degree of security. It may well be that certain groups (such as immigrants) are subject to higher degrees of suspicion and so are targeted more frequently, while the security offered may not be to the groups whose privacy is diminished. This risks an imbalance in society in which the vulnerable become more vulnerable in order for the privileged to retain their status.

In the third place, it is not always the case that people prefer to have security over privacy. Wars have been fought over the right to maintain a liberal democratic way of life, a central part of which, as we have seen, is the respect for privacy. Thus people have surrendered their lives in order that others may have privacy, and all that that entails.

The second argument states that if you have done nothing wrong, then you have nothing to fear from surveillance. This argument also fails on several levels. Firstly, it assumes that there is an objective standard of ‘wrong’ which will never change. However, in Weimar Germany it was not ‘wrong’ to be Jewish, but within 10 years and the rise of Nazism it became ‘wrong’ in the eyes of the new leaders of Germany. Hence in practice there is frequently a political dimension to what is deemed wrong. This may be true in the corporate world as well, in which discrimination against homosexuality or certain political leanings can cost a person their job.

Secondly, the argument places an unwarranted degree of trust in the surveillant authority. This might be reasonable if that authority were known to be infallible, but that is never the case. Abuses by the state in the form of police or intelligence agencies overstepping agreed boundaries are widely known in most liberal democracies, the

revelations by Edward Snowden being the most recent. Indeed, one of the values of a democratic system is that it recognizes the potential for such abuses and provides a means of accountability so that the public can react accordingly in the event of abuses being uncovered. Likewise, as referenced above, corporations can similarly overstep the boundaries of reasonable surveillance in pursuit of whistleblowers or profit from exploiting personal data. In the corporate world, though, accountability is generally a matter of legality. Hence, when there are not enough laws protecting the privacy of employees or customers, corporations have a large degree of discretion in how they act.

Thirdly, the argument implies that if I do have something to hide then I must have done something wrong, but this is clearly not the case. In closing the toilet door, drawing the curtains at night, or writing in a diary, I am not doing anything wrong. You might even know (or be able to infer) what I am doing. Nonetheless, it is valuable to me for the reasons explored above that I am able to conduct these activities in private.

Hence, both of these popular arguments are deeply flawed and overlook serious issues that arise with a lack of privacy. This is significant when it comes to evaluating decisions regarding surveillance in society. These arguments may be employed in good faith by those in favour of increasing surveillance under certain circumstances, such as a recent terrorist atrocity or a whistleblowing-related leak. However, the flaws in the arguments demonstrate that they should not be used in support of increasing surveillance. Rather, they should be dismissed in favour of more robust reasons for, or against, increasing surveillance at the expense of privacy.

CONCLUSION

In this paper we have considered the recent history of scholarship on privacy in terms of both legal and philosophical arguments. We then turned to look at contemporary debates in privacy to see that these revolve around the precise nature and value of privacy, as well as what is entailed by privacy. This led to a consideration as to whether there is a right to privacy, which we saw was arguably reasonable, although such a right is not absolute nor entirely inviolable. Finally, we turned to two popular arguments regarding privacy and the surveillance, and saw that both of these overlooked serious problems, contained dangerous assumptions, and had undesirable consequences.

REFERENCES

Allen, A., 2011. Unpopular Privacy: What Must We Hide? OUP USA, New York, N.Y.

Allen, A.L., 2008. The Virtuous Spy: Privacy as an Ethical Limit. The Monist 91, 3–22.

Allen, A.L., 1999. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. Conn. L. Rev. 32, 861.

Allen, A.L., 1998. Coercing Privacy. Wm. & Mary L. Rev. 40, 723.

Allen, A.L., 1988. Uneasy Access: Privacy for Women in a Free Society. Rowman & Littlefield, Totowa, N.J.

Benn, S., 1971. Privacy, freedom, and respect for persons, in: Pennock, J., Chapman, R. (Eds.), Nomos XIII: Privacy. Atherton Press, New York.

Brandom, R., 2018. Even if you're not signed up, Facebook has a shadow profile for you [WWW Document]. The Verge. URL https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (accessed 2.20.19).

Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.

Carpenter v. United States, 2018.

Dhawan, S., 2009. "Privacy is Dead - Get Over It!" [WWW Document]. TheCourt.ca. URL http://www.thecourt.ca/privacy-is-dead-get-over-it/ (accessed 12.9.18).

Directive 95/46/EC, 1995. , 281.

Doyle, T., 2009. Privacy and Perfect Voyeurism. Ethics and Information Technology 11, 181–189.

Duhigg, C., 2012. How Companies Learn Your Secrets. The New York Times.

(EU) 2016/679, 2016. , (EU) 2016/679.

EU Parliament, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L.

EU Parliament, 1995. Directive 95/46/EC of the European Parliament and of the Council.

Fitzgerald, A.E., 1972. The High Priests of Waste. W. W. Norton Limited.

Grabenwarter, C., 2014. European Convention on Human Rights, in: European Convention on Human Rights. Nomos Verlagsgesellschaft mbH & Co. KG.

Hill, K., 2017. How Facebook Figures Out Everyone You've Ever Met [WWW Document]. Gizmodo. URL https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691 (accessed 2.20.19).

Hosein, G., 2014. On Just Surveillance. Surveillance & Society 12, 154–157.

Inness, J.C., 1996. Privacy, Intimacy, and Isolation, New Ed edition. ed. Oxford University Press, New York.

Kant, I., 1969. Critique of Pure Reason, Unabridged. ed. Bedford Books.

Katz v. United States, 1967. , U.S.

Lever, A., 2013. Privacy: Restrictions and Decisions. Newsletter of the American Philosophical Association: Philosophy and Law 13, 1–7.

Lever, A., 2007. Mill and the Secret Ballot: Beyond Coercion and Corruption. Utilitas 19, 354–378. https://doi.org/10.1017/S0953820807002634

Lever, A., 2005. Feminism, Democracy and the Right to Privacy (SSRN Scholarly Paper No. ID 2559971). Social Science Research Network, Rochester, NY.

Locke, J.L., 2010. Eavesdropping: An Intimate History. OUP Oxford.

Lord, N., 2018. What is the Data Protection Directive? The Predecessor to the GDPR [WWW Document]. Digital Guardian. URL https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr (accessed 12.9.18).

Lovett, F., Pettit, P., 2009. Neorepublicanism: A Normative and Institutional Research Program. Annual Review of Political Science 12, 11–29. https://doi.org/10.1146/annurev.polisci.12.040907.120952

Lyon, D., 2001. Facing the Future: Seeking Ethics for Everyday Surveillance. Ethics and Information Technology 3, 171–181.

Macnish, K., 2018. Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. Journal of Applied Philosophy 35, 417–432. https://doi.org/10.1111/japp.12219

Macnish, K., 2017. The Ethics of Surveillance: An Introduction, 1 edition. ed. Routledge, London : New York.

Macnish, K., 2014. Just Surveillance? Towards a Normative Theory of Surveillance. Surveillance and Society 12, 142–153.

Marx, G.T., 2014. Toward an Imperial System of Surveillance Ethics. Surveillance & Society 12, 171–174.

Marx, G.T., 1998. Ethics for the New Surveillance. The Information Society 14, 171–185.

Mill, J.S., 2006. On Liberty and the Subjection of Women. Penguin Classics.

Moore, A., 2013. Coercing Privacy and Moderate Paternalism: Allen on Unpopular Privacy. Newsletter of the American Philosophical Association: Philosophy and Law 13, 10–14.

Moore, A., 2008. Defining Privacy. Journal of Social Philosophy 39, 411–428.

Moore, A., 2003. Privacy: Its Meaning and Value. American Philosophical Quarterly 40, 215–227.

Moore, A.D., 2015. Waiving privacy rights: Responsibility, paternalism, and liberty.

Moriarty, E., 2011. Did the Internet Kill Privacy? [WWW Document]. URL https://www.cbsnews.com/news/did-the-internet-kill-privacy/ (accessed 1.10.19).

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

Olmstead v. United States, 1928.

Palm, E., 2014. Conditions under which Surveillance may be Ethically Justifiable—Remarks on Kevin Macnish's proposed normative theory of surveillance. Surveillance & Society 12, 164–170.

Pettit, P., 2014. Just Freedom: A Moral Compass for a Complex World. W. W. Norton & Company, New York.

Pettit, P., 2001. Republicanism: A Theory of Freedom and Government, New Ed edition. ed. Oxford University Press, U.S.A., Oxford.

Rachels, J., 1975. Why Privacy is Important. Philosophy and Public Affairs 4, 323–333.

Regan, P., 2002. Privacy as a Common Good in the Digital World. Information, Communication & Society 5, 382–405.

Regan, P.M., 1986. Privacy, Government Information, and Technology. Public Administration Review 46, 629–634. https://doi.org/10.2307/976229

Scanlon, T.M., 1975. Thomson on Privacy. Philosophy and Public Affairs 4, 315–322.

Solove, D.J., 2008. Understanding Privacy. Harvard University Press.

Solove, D.J., 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review.

Solove, D.J., 2002. Conceptualizing Privacy. California Law Review 90, 1087–1155.

Stoddart, E., 2014. Challenging 'Just Surveillance Theory': A Response to Kevin Macnish's 'Just Surveillance? Towards a Normative Theory of Surveillance.' Surveillance & Society 12, 158–163.

Thomson, J.J., 1975. The Right to Privacy. Philosophy and Public Affairs 4, 295–314.

Tobitt, C., 2018. Observer's Carole Cadwalladr: I became a 'news slave' in pursuing Cambridge Analytica data harvesting scoop – Press Gazette. the Guardian.

United Nations, 1948. The Universal Declaration of Human Rights [WWW Document]. URL http://www.un.org/en/documents/udhr/index.shtml (accessed 6.13.11).

United States v. Jones, 2012.

Walzer, M., 1984. Spheres Of Justice: A Defense Of Pluralism And Equality by Michael Walzer. Basic Books.

Warren, S.D., Brandeis, L.D., 1890. The Right to Privacy. Harvard Law Review 1–19.

Westin, A.F., 1967. Privacy and Freedom. Athenaum, New York, NY.