No cover image available

The Oxford Handbook of Digital Ethics

Carissa Véliz (ed.)

https://doi.org/10.1093/oxfordhb/9780198857815.001.0001

Published: 2021 **Online ISBN:** 9780191890437 **Print ISBN:** 9780198857815

CHAPTER

The Surveillance Delusion

Carissa Véliz

https://doi.org/10.1093/oxfordhb/9780198857815.013.30 Pages C30.P1–C30.N7

Published: 19 December 2022

Abstract

This chapter explores the ethics of surveillance in the digital age by assessing its lights and shadows. After assessing the consequences of surveillance for freedom and democracy, it argues that we should resist *the surveillance delusion*: the assumption that surveillance has no significant moral costs. Under the surveillance delusion, only the benefits of surveillance are considered, and, as a result, surveillance is taken to be a convenient solution to problems that could be solved through less intrusive means—all without realizing that surveillance itself may be creating more weighty problems in the long run than the ones it is solving.

The privacy landscape in the first two decades of the twenty-first century is radically different than that of the last two decades of the twentieth century. In 1980, an ordinary person was unlikely to be subjected to extensive corporate or governmental surveillance. Even though there have been censuses since the end of the eighteenth century, tax records go back to the early twentieth century, and private-sector databases have been a privacy threat since at least the 1970s (Solove 2001), the extent of surveillance was limited by friction that is now largely being overcome by digital technologies. In the 1980s, some personal data was collected for corporate purposes, but companies didn't have the means to track every single person throughout their day, and the ability to buy and integrate different databases wasn't a few clicks away. There were some CCTV cameras on the street but fewer than today and with no facial recognition. The only reason why someone could end up being subjected to serious governmental intrusion in liberal democracies was if they were criminal suspects. Even then, the amount of data the police could get on them is nowhere near the amount of data that is collected about ordinary citizens today.

Our financial transactions, online searches, movements, communications, relationships, and interactions with governments and businesses all generate personal data that is being collected, sold, and bought by data brokers, corporations, and governments interested in profiling individuals. The commodification of personal data brings with it promises: greater safety, economic gain, and scientific and technological advancements. The concomitant loss in privacy, however, has severe costs that, arguably, are not being taken seriously enough, judging by the constant expansion of surveillance. Surveillance puts people at risk of suffering discrimination, exploitation, and other kinds of abuse such as extortion. Furthermore, it pushes society into a culture of exposure that can breed conformity and jeopardize democracy.

The first section gauges the breadth and depth of surveillance in the digital age. In the second section, I assess the role of consent in surveillance practices. The third section discusses whether current levels of surveillance amount to mass surveillance and to what extent that is ethically problematic. In the fourth section, I sketch the costs of surveillance in terms of risks, harms, and wrongs. The fifth section explores whether ubiquitous surveillance can be justified for the purposes of security. In the sixth section, I investigate whether surveillance is justifiable as a business model. In the seventh section, I assess whether ubiquitous surveillance can be justified for the purposes of technological advancement. In the eighth section, I analyse the relationship between surveillance, freedom, and democracy. Finally, in the ninth section, I conclude by hypothesizing that the nature of the costs of surveillance often leads people to fall into the trap of the *surveillance delusion*: the assumption that surveillance has no significant moral costs. Under the surveillance delusion, only the benefits of surveillance are considered, and, as a result,

surveillance is taken to be a convenient solution to problems that could be solved through less intrusive means—all without realizing that surveillance itself may be creating more weighty problems in the long run than the ones it is solving.

The breadth and depth of surveillance in the digital age

The amount of personal data collected about people around the world has been consistently increasing during the past two decades on account of a few factors.[1] First, the development of data analysis tools has made it easier than ever to collect personal data. Second, as we interact more than ever with computers (and computers interact with us), more personal data than ever is created. Third, regardless of whether institutions are in the business of technology, every institution has an incentive to collect personal data because it can be sold to third parties—personal data has become an easy way to earn money. The personal data economy—the buying and selling of personal data—has given rise to companies that specialize in the commodification of personal data: data brokers. These companies aim to have a file on every internet user, which they then sell to insurance companies, banks, prospective employees, governments, etc.

Some of that data will have been offered by users with various degrees of voluntariness. For example, people routinely share their email addresses and phone numbers with companies whenever they purchase something and have it delivered to their home. What they might not realize is that those companies are likely to share that information with hundreds of other companies, who will then use it to make sensitive inferences. While someone might not think that sharing one's music tastes with companies is sensitive data, companies often take non-sensitive data and turn it into sensitive data through inferences, for example, inferring sexual orientation from music preferences (Kosinski et al. 2013).

One of the distinctive data risks of the digital age is the aggregation of data across databases. Before data was digitized, it wasn't as dangerous to surrender personal data to very different institutions because the chances of those databases being aggregated was slim. Digitization and the internet have made it easy to share data. As the amount and depth of public databases increases, our privacy is more at risk because it becomes easier to 'join the dots' and learn more about people than they were willing to share.[2]

For example, in 2006, Netflix published 10 million movie rankings by half a million customers as part of a challenge for people to design a better recommendation algorithm. The data was supposed to be anonymous, but researchers at the University of Texas at Austin managed to re-identify people by comparing rankings and timestamps with public information in the Internet Movie Database (IMDb). If someone saw a movie on a particular night, liked it on Netflix, and then rated it on IMDb as well, researchers could infer that was the same person. Movie preferences can reveal sensitive information such as sexual orientation. A lesbian mother sued Netflix for placing her at risk of being outed (Singel 2009). The danger of exposure through aggregation and inferences has become all the more pungent since data brokers took it upon themselves to aggregate as much data as possible about each individual.

The extent of data collection on every internet user is astonishingly broad. A typical data broker will have thousands of data points about every person, including age, gender, education, employment, political views, relationship status, purchases, loans, net worth, vehicles owned, properties owned, banking and insurance policies details, likelihood of someone planning to have a baby, social media activity, alcohol and tobacco interests, casino gaming and lottery interests, religion, health status, and much more (Melendez and Pasternack 2019).

To put that into perspective, the Stasi, the security service of East Germany, notorious for its surveillance capabilities, held much less data on its citizens. They had one spy or informant for every sixty-six citizens (Koehler 1999: 9) and managed to have files on little more than one-third of the population (Cameron 2021). Today, with a significant proportion of people volunteering private information on social networks and carrying a smartphone in their pockets, governments can have a file on every single citizen with substantially more data than the Stasi ever had.

One might think that the comparison with the Stasi is misleading because that was government surveillance and the kind of surveillance we face today is mostly corporate, which can be thought to be less dangerous. Government surveillance is often thought to be more worrisome on account of the special powers that governments hold (e.g. to arrest people). Data collection and trades have become so ubiquitous, however, that it is unhelpful to distinguish between corporate and governmental surveillance as data collected by the

former is shared to the latter and vice versa (Véliz 2020: 27–45). Even when corporations refuse to give up data to governments (as in the case of Apple refusing to help the FBI hack into a dead criminal's phone in 2016), governments often have the ability to hack into data themselves or to hire the services of someone who will do it for them (which is exactly what happened in the Apple case) (Yadron 2016).

Most countries don't have the means to develop surveillance and hacking tools so they buy them from cyberweapons manufacturers (Schneier 2018: 65). Countries routinely use the tech giants to outsource surveillance. Palantir, Amazon, and Microsoft, for instance, provided tools that aided the Trump administration in putting under surveillance, detaining, and deporting immigrants (Levin 2018). Court records in the United States show that investigators can ask Google to disclose everyone who searched for a particular keyword (as opposed to asking for information on a known suspect) (Ng 2020). In short, any personal data that is collected by a company can end up in the hands of the police (Morrison 2021).

In some cases, corporate surveillance can be used to bypass official policies. In 2018, John Roberts, Chief Justice of the Supreme Court in the United States, authored a majority opinion ruling against the government obtaining location data from mobile phone towers without a warrant. Unsatisfied with that decision, the Trump administration bought access to a commercial database that maps the movements of millions of mobile phones in the United States. Given that such data is for sale from data brokers, the government didn't need a warrant to get it. By outsourcing surveillance to private companies, the government found a way to bypass a Supreme Court ruling (Cox 2020). In another example, in its pursuit of two suspects, the United States asked Mexico to use a facial recognition system made by a Chinese company that had been blacklisted by the US government (Hill 2021).

The flow of information goes both ways: governments also collect personal data that they pass on to businesses—sometimes for a profit. Data about millions of patients in the National Health Service in the United Kingdom has been sold to pharmaceutical companies, for example (Helm 2019).

In short, the breadth and depth of data collection and data sharing in the digital age is more vast than ever before.

The role of consent in surveillance practices

It is intuitive to think that if losses of privacy are consented, there is no harm done.[3] Companies often claim that their surveillance practices are unproblematic because users give their consent when agreeing to their terms and conditions. However, consent in the context of the data economy is an ethically questionable practice at its best.

The notion of informed consent comes from medical ethics. In that context, it is a tool to honour and protect patients' autonomy. Autonomy is the ability and right of adults to choose their own values and act accordingly. If patients are to be treated as ends in themselves, according to the Kantian categorical imperative, that means we must recognize that they have their own priorities and objectives and that the medical profession has no right to interfere with their desires. That is why doctors cannot do research on patients or intervene in their bodies without their permission.

Unfortunately, the practice of consent does not travel well to the data context. While the medical profession is supposed to be set up to aid patients, companies are typically wanting to profit from their users. This means that terms and conditions are written to protect companies—not ordinary people—from liability. Terms and conditions are usually unreasonably long, non-negotiable, and can change at any time without previous warning.

Furthermore, even if terms and conditions were short and negotiable, there is arguably no such thing as *informed* consent in the context of the data economy. Data implications are notoriously difficult to understand, often impossible. Neither the people who wrote the privacy policy nor the programmers who wrote the code for the algorithms that analyse data know what kind of inferences might be drawn from the data they get from users or where that data might end up once it gets sold. If no one knows, the user cannot be informed in any meaningful sense.

A third challenge for consent in data contexts is that it is often hard or impossible to ask all relevant people for consent. For example, if someone does a DNA test, they might be consenting, but their parents, siblings,

children, and distant kin are not giving their consent. Most personal data either contains data about other people or can be used to infer data about other people, such that it is unclear whether an individual has the moral authority to consent to giving up their data.

Finally, consent may not be voluntary. Very often, people do not have a meaningful choice in using technological tools that are necessary to be full participants of society, and terms and conditions do not allow for any kind of negotiation.[4]

Thus, while there may be a role for consent in surveillance practices, that role is not as broad as it might be imagined, and someone giving consent to be put under surveillance does not automatically mean that such a practice is ethical.

Does bulk data collection amount to mass surveillance?

One important debate in the surveillance literature is whether such vast bulk collection of personal data equals mass surveillance. Both surveillance companies and intelligence agencies have an interest in defending the view that bulk collection of personal data is not an invasion of privacy as it makes what they do sound less problematic.

When Steven Levy interviewed National Security Agency (NSA) officials, he realized that 'looking at the world through [NSA's] eyes, there is no privacy threat in collecting massive amounts of information' (Levy 2014). The thought is, roughly, that even though everyone's data is being collected on a mass scale, that doesn't amount to mass surveillance because that data rarely gets accessed. What it is exactly that people mean by 'access' is unclear and much depends on it, but one example is that, even if intelligence agencies have plentiful data about you, if you are not interesting to them, the chances are that no human agent will ever look at that data. In this vein, Mark Pythian writes: 'If innocent people are unaware that their communications have been intercepted, stored, and filtered out by computer—thus not ever seen by a human analyst—then the intrusion is potential, not actual, and the potential for harm to the individual negligible' (Omand and Phythian 2018: 24–25). Similarly, David Omand argues that bulk access to data does not amount to mass surveillance because, for most of the data, no human analyst sees and logs it for future action (Omand and Phythian 2018: 150).

Those who consider that collecting information is privacy-invasive tend to think about either privacy or the right to privacy as a matter of control.[5] To them, if someone loses control over their data, that amounts to either losing privacy or having their right to privacy violated. Those who think that data collection is not a privacy worry tend to think of privacy or the right to privacy as a matter of access: as long as the data does not get accessed, there is no privacy invasion.[6] Kevin Macnish, for example, argues that loss of control over our personal data can make us *feel* vulnerable and can make us more vulnerable through increasing the risk that the personal data might be accessed one day. Despite this increased vulnerability, argues Macnish, as long as the data is not accessed, there is no privacy violation (Macnish 2016).

Data collection certainly risks our privacy, and that is partly what is wrong with it. But that is not the whole story. Suppose an intelligence agency like the NSA (in the United States) or Government Communications Headquarters (commonly known as GCHQ, in the United Kingdom) comes to an agreement with you: they will collect all your data, but if you never criticize the government, they will never access it. Suppose further that you can trust this promise and that the agency can guarantee without a doubt the safety of your data such that, if you never criticize the government, your data is as safe as if it had never been collected. There is still some wrong being committed here. One might be tempted to think that it is an abuse of power, but many rights violations by government agencies are abuses of power: murder, unjustified incarceration, etc. What is characteristic of this particular abuse of power is that it attempts against our privacy, and the best way to capture that is by explaining it in terms of our right to privacy. From here on, I will therefore assume that the collection of personal data is a form of surveillance.

The risks, harms, and wrongs of surveillance

If this assessment is right, given that surveillance implies a significant intrusion, it can only be justified if its benefits outweigh its costs. Even if someone were to argue that bulk data collection does not amount to mass surveillance and does not violate privacy, that surveillance has costs is undeniable.

At the very least, the cost of surveillance is an increased risk of exposure. Personal data is dangerous because it is sensitive, highly susceptible to misuse, hard to keep safe, and desired by many—from criminals to insurance companies and intelligence agencies. The more data is collected, the longer it is stored, and the more it is passed on from one institution to the next, analysed, and aggregated with other data, the more likely it is that it will end up being misused. Examples of data misuse include neglect (i.e. when the data is not kept safe and ends up being leaked), exposure, and unlawful discrimination.

The kind of surveillance that is common in the digital age therefore entails, at the very least, a *risk*. It sometimes also entails a *harm*, for example, when risks materialize and there is a case of exposure or discrimination. Finally, surveillance incurs the infringement or violation of the right to privacy. When a privacy invasion is justified, it amounts to a right infringement; if the invasion is unjustified, then it amounts to a violation of the right to privacy and therefore a *wrong*.

The requirements of ethical surveillance: Necessity and proportionality

It is widely accepted that what it takes for surveillance to be ethical is that it be necessary and proportionate (Hadjimatheou 2014; Macnish 2015; Brown and Korff 2009). Given that surveillance has costs, it has to be *necessary* in that comparable beneficial results cannot be achieved by less intrusive or harmful methods. The moral concept of *proportionality* refers to a moral constraint on actions that cause harm. For an act that causes harm to be proportionate, it must be done in the pursuit of some valuable goal against which the harms are weighed (McMahan 2009: 19). If benefits outweigh harms, risks, and wrongs (if the bad that an act creates is less than the bad it prevents), then the act is proportionate. An implicit condition of proportionality is that surveillance has to be effective. If surveillance has costs and no benefits because it is not effective (it doesn't do what it's supposed to do), then it can hardly be justified (Véliz 2017, forthcoming).

Proportionality is concerned with comparing the consequences of doing an act with the consequences of not doing it. Necessity is concerned with comparing what will happen if an act is done with what will happen if alternative acts are done that are also means of achieving the same end. Proportionality is concerned with the question: are the bad effects of this act such that the good effects cannot be justified? Necessity, in contrast, asks: what is, morally, the best means for achieving certain ends?

The idea of proportionality in surveillance is not foreign to law and public policy. The Investigatory Powers Bill in the United Kingdom includes proportionality among the considerations to be taken into account under general duties in relation to privacy. In 2014, 500 organizations and experts worldwide signed the International Principles on the Application of Human Rights to Communications Surveillance, which includes the principle of proportionality (Schneier 2015: 168).

There are three purported benefits that are often used to justify surveillance: security, economic gain, and technological advancement. I will discuss each of these in turn and assess whether digital surveillance is proportionate and necessary to achieve the benefits pursued.

Surveillance and security

The expansion of surveillance at the end of the twentieth and the beginning of the twenty-first centuries was tied to a concern for security. In the United Kingdom, a so-called Ring of Steel was created after the Irish Republican Army (IRA) exploded truck bombs in the City of London in the early 1990s (Carlile 2004). The Ring of Steel is a zone of cameras built around the financial district that got gradually expanded and updated and that in the early 2000s turned Britain into the country in the world with the most video surveillance (that place has now been superseded by China and the United States, in that order) (Carlile 2004; Brandl 2021). More recently, in 2016, the Investigatory Powers Act introduced new governmental powers of bulk collection of data for the purposes of security.

In the United States, it was also the threat of terrorism that motivated the expansion of surveillance. In 2000, the Federal Trade Commission had recommended that the United States Congress regulate the data economy. But after 9/11, the US government saw an opportunity to make a copy of all the data being collected by the corporate world and use it for the purposes of national security. Unbeknownst to citizens, shortly after the attacks, a secret system of mass surveillance was implemented with the objective of increasing security. With the passing of the Patriot Act, six weeks after the terrorist attacks, the Federal Bureau of Investigation (FBI) was allowed to issue 'national security letters', a form of subpoena that is not subject to judicial oversight and allows spying into the private lives of people (phone records, bank accounts, web searches, and credit card purchases) who might not even be considered suspects (Wright 2008). Similar trends followed in other countries such as France.

There are a few arguments that can be offered in favour of ubiquitous surveillance for the purposes of security. Although mass surveillance tends to carry with it a negative connotation, Katerina Hadjimatheou has argued that, first, untargeted surveillance is less likely to stigmatize those who are watched because everyone is being watched. However, arguably, when criminal suspects are watched covertly (through targeted surveillance, the alternative to mass surveillance), they are not being stigmatized because no one knows about the surveillance.

Second, Hadjimatheou argues, mass surveillance is likely to be a less intrusive privacy measure if it's overt because it allows people to adapt their expectations and plan accordingly. The example she gives is how, when people know there will be surveillance at airports, they can make sure not to carry sensitive objects in their hand luggage (2014: 204). However, once surveillance becomes truly ubiquitous, there is no avoiding it and therefore no planning accordingly. When a surveillance apparatus follows our every step and keystroke along the day, altering our behaviour amounts to potentially drastic self-censorship. Not carrying sensitive objects in our hand luggage might not be a big inconvenience, but changing what we search for online, whether we go to a protest, or what we say to our loved ones out of fear of surveillance has serious implications for individuals and democracy (de Bruin 2010; Gavison 1980; Véliz 2020), as we will see later.

Third, Hadjimatheou argues, indiscriminate surveillance is likely to be more efficient as a deterrent for wrongdoing (Hadjimatheou 2014: 189, 197). Whether this argument succeeds will depend, first, on how effective mass surveillance is at preventing crime and, second, how much wrongdoers are willing to lose; in the case of extremist terrorists who are willing to give up their lives, it may not act as much of a deterrent.

Perhaps the most powerful argument in favour of mass surveillance is that we must subject ourselves to surveillance as part of a duty to protect one another from rights violations. In some cases, it is permissible to deliberately harm a person as a way to enforce a 'duty to protect third parties from wrongful harm—subject, of course, to considerations of necessity, effectiveness and proportionality' (Fabre 2022: Ch. 9). As mentioned before, terrorism has been front and centre in the defence of surveillance.

A necessary condition for surveillance to be justified is that it be effective. Whether mass surveillance is effective is a contentious issue. While David Anderson found that bulk collection of data helped foil criminal plots in the United Kingdom (Anderson 2016), none of the many oversight committees or investigations in the United States have found it effective (Clarke et al. 2013: 104, 120; Bergen et al. 2014: 1; Savage 2015a; 2015b: 162–223; 'Report on the President's Surveillance Program' 2009: 637; Isikoff 2013). Although my own conclusion is that it is very doubtful whether mass surveillance will ever be an effective method of preventing terrorism, I will assume effectiveness in what follows for the sake of argument.

Once effectiveness has been established or assumed, surveillance still needs to be necessary and proportionate to be justified. Together, both requirements serve the goal of making sure we are better off

with mass surveillance than without it.

There are serious doubts about whether mass surveillance for the purposes of ensuring security can be proportionate. The wrong of mass surveillance is significant, given that the right to privacy of the whole of the population is violated. With that wrong come concomitant risks and harms. Among them are chilling effects: the possibility of authorities treating all citizens like criminal suspects and going on fishing expeditions in search of illegality and the risk of that data being hacked, leaked, or seriously misused in the future.

Similarly, there are doubts about whether mass surveillance is necessary, and, if it is unnecessary, it can hardly be proportionate. There is reason to think that targeted surveillance is superior to mass surveillance as well as less intrusive. With targeted surveillance, the police or intelligence agencies must first get a tip. The tip usually comes from the community or from family members, but it can also come from informants or relevant information can turn up from other criminal investigations. Once there is good reason for suspicion, investigative authorities present the evidence to a judge, who must decide whether there is enough evidence for suspicion to order a warrant for surveillance to take place. This system works surprisingly well. Because police officers will have to go back to the same judges for warrants in future cases, they are careful to build trust with them and ask for warrants only when it is quite likely they will find something. In fact, police find at least some of the evidence they had expected in more than 80 per cent of cases (Solove 2011: 130).

Experience since 9/11 suggests that targeted surveillance is more effective than mass surveillance in preventing terrorism, which supports the conclusion that bulk surveillance is neither necessary nor proportionate for achieving our counterterrorist goals. The major technical problem with mass surveillance seems to be that which characterizes it: the extent of the collection of data. The sheer quantity of information adds irrelevant data about innocent people and obscures what would be significant tips from targeted surveillance. Mass surveillance adds hay to the haystack and makes it all the more difficult to find the needle.

Security expert Bruce Schneier has argued that bulk collection and data-mining are inappropriate tools for finding terrorists for three reasons (2015: 136–140). First, error rates are unacceptably high. When we use data-mining to target people for something relatively innocuous such as fashion advertisement, mistakes can be tolerated more easily as getting advertisements for clothes we do not want to buy is usually not too problematic. But when data-mining is used to look for terrorists, the lives and freedom of potentially innocent people are at stake, and our tolerance for mistakes should be low.

The second reason for the inappropriateness of data-mining techniques for investigating terrorism is that terrorist attacks are unique. There was no way of predicting that pressure-cooker bombs would be used in the Boston Marathon attack (Schneier 2015: 138), or that someone might put a bomb in his shoe, or that people would try liquid explosives, or that someone might kill people with a cargo truck in Nice. Jeff Jonas, an IBM research scientist, and Jim Harper, the director of information policy at the Cato Institute, argue that ‘terrorism does not occur with enough frequency to enable the creation of valid predictive models’ (Jonas and Harper 2006: 8).

The third problem is that terrorists will be trying to avoid detection, making it harder for them to be caught in the very broad nets cast by intelligence agencies.

A final problem beyond necessity and proportionality is the concern that mass surveillance can end up jeopardizing national security due to both internal and external risks. Internal risks include the possibility of a future bad government taking control of the architecture of surveillance and using it to become an authoritarian regime. External risks include the possibility of an adversary country hacking into sensitive systems and using personal data for intelligence or even military purposes. These risks illustrate a ‘real and unavoidable’ contradiction identified by Timothy Garton Ash when governments spy on their own citizens, thereby infringing the freedom they are supposed to defend: ‘if the infringement goes too far, it begins to destroy what it is meant to preserve’ (Garton Ash 1997: 236). We will return to this issue in the conclusion.

Even if we agreed that it’s not worth implementing ubiquitous surveillance for the sake of security, there are those who might think that surveillance is justified for the sake of economic gain.

Surveillance and economic gain

The commodification of data, often called the data economy, has become a remarkably profitable industry. 'The world's most valuable resource is no longer oil, but data', read an *Economist* article in 2017. A significant part of the data market is tied to personalized advertising, which uses personal data to show relevant ads to people. Advertising is the main way the internet funds itself, and most advertising online is personalized. That makes personal data one of the most valuable kinds of data. What used to be considered wiretapping and the purview of police has become a mainstream business model.

Personalized advertising is often organized around bidding. Real-time bidding (RTB) sends a user's personal data to interested advertisers, often without their permission. Suppose Amazon gets that data and recognizes them as a user who has visited their website before in search of a book. They might be willing to pay more than others to lure them into buying that book because they are confident they wants it. And that's how they get shown an Amazon book ad. In that process, however, very personal data, such as sexual orientation and political affiliation, might have been sent to dozens or even hundreds of possible advertisers without the user's knowledge or consent. And those companies get to keep that personal data, which often gets sold on to other third parties (ICO 2019).

Another crucial piece of the puzzle of the data economy are data brokers. Whenever there is personal data collected, there is a good chance it will end up in the hands of data brokers. Data brokers aim to have a file on all internet users. They then sell those files to prospective employers, insurance companies, governments, and anyone else willing to buy the data. A company like Experian, for example, aggregates data on over a billion people and businesses, including 235 million US consumers. Axciom has more than 10.000 data points on every one of 2.5 billion consumers in 62 countries (Melendez and Pasternack 2019).

While the data economy is highly profitable at the time of writing, it is questionable whether its benefits outweigh its costs for society. With wealth inequality increasing around the world (Alvaredo et al. 2018), there is no evidence to think that profits to companies like data brokers trickle down to the rest of society. Unlike the big companies of the past, data brokers are not companies that employ a large number of people. While a car manufacturer employs hundreds of thousands of people (e.g. Volkswagen employed 665,000 people in 2020, according to Statista), a data broker typically employs only a few thousand (e.g. Experian, one of the largest data brokers, employs around 16,000 people, according to its website).

In turn, the societal harms and risks of an economy founded on surveillance are significant. Data brokers make it very hard to police anti-discrimination laws. When anyone can acquire sensitive information about others without any kind of supervision, it is hard to make sure that companies are not discriminating against people for their political tendencies, their sexual orientation, or their health status, for example. Often, when people are treated on the basis of their data by both private and public institutions, they cease to be treated as equal citizens (Véliz 2020).

The risk that sensitive data will be hacked and misused is also high. In September 2017, Experian announced a cybersecurity breach in which criminals accessed the personal data of about 147 million US citizens. The data accessed included names, social security numbers, birth dates, addresses, and driver's licence numbers. It is one of the biggest data breaches in history. In February 2020, the United States Department of Justice indicted four Chinese military people on nine charges related to the breach (which China has so far denied). That foreign countries are hacking sensitive data alerts us to a further risk in national security.

Through data acquired from a location data broker, journalists in the *New York Times* managed to find the location of the President of the United States through correlating his public schedule to a phone that belonged to a Secret Service agent (Thompson and Warzel 2019). With the same database, the reporters were also able to identify and follow military officials with security clearances and law enforcement officers, among others.

There are also concerns about how the data economy incentivizes the design of algorithms on social media that lead to misinformation and the polarization of society. Social media companies want people to stay on their platforms for as long as possible because that is how they can collect as much personal data from them as possible and show them as many ads as possible. Unfortunately, the content that is most engaging is often toxic content like misinformation and heated political debates that end up polarizing citizens into extreme positions (Wylie 2019). For an argument on why there is too much privacy on social media today, see Marmor, this volume. For a response to that argument, see Véliz (2021).

Finally, there is a concern that the personalized ads market is a financial bubble. Microtargeting is much less effective and accurate than it's made out to be and too expensive for it to be worth it (Edelman 2020; Hwang 2020). The market is so opaque (because real-time bidding is abstract and it is difficult to verify that a particular ad that has been bought is reaching its intended audience and having an effect) that it allows for errors in valuation and click fraud. Click fraud uses automated scripts or paid humans in 'click farms' to click on an ad, but there is no consumer viewing that ad (Hwang 2020: 84). And part of why the market is so opaque is because ads are personalized; if everyone saw the same ad, it would be easier to verify that it's being shown. Forrester Research estimated that, in 2016, as much as 56 per cent of all the money spent on ads in the United States was lost to fraud or unviewable ads (Bidel et al. 2017). The worry is that, once the businesses that have bought personalized ads realize that they have been paying for something that is not worth it, the bubble will burst, and we will find ourselves in the midst of a financial crisis similar to the 2008 one.

Given that the data economy has increased inequality, harmed equality, is a threat to national security, can lead to the polarization of society and to disinformation, and is risking a financial crisis, it doesn't seem like surveillance is a justified business model. Ubiquitous surveillance as a business model is not necessary. Humanity had already achieved a high level of wealth before the data economy came along. One of the main reasons why so much personal data is collected online is to fund internet companies like Facebook and Google, but those companies could be funded through alternative business models, including subscription models, and through advertising that does not depend on personal data. Contextual advertising, for instance, shows ads to people based on what they just searched for without needing to know anything else about them. Given that it is not necessary and that its advantages can be achieved through less costly means, surveillance as a business model is not proportionate either.

Surveillance and technological advancement

A third common reason to justify the collection of personal data is for the purposes of technological and scientific advancement. In particular, it is often thought that personal data is needed in abundance for the purposes of training artificial intelligence (AI). By the mid-1980s, AI researchers had moved away from symbolic AI (based on rules of logic) and had started making important progress in neural networks (based on statistical models), which eventually led to a flourishing of machine-learning research and applications.[7] One of the particularities of machine-learning algorithms is that they need huge amounts of data.

In many cases, however, the most useful data to train AI is not personal data. Personal data often has a short expiry date (people move houses, they change their job, their tastes evolve, etc.), and it can often be less accurate than other kinds of data, partly because it is difficult (if not impossible) to place people intro discrete categories (Crawford 2021: Ch. 4). A poster child of AI is AlphaZero, an algorithm developed by Google's DeepMind that plays the ancient Chinese game of Go. AlphaZero was trained exclusively through playing against itself without any external data, let alone personal data. Another example of AI using data that is not personal is researchers at the Massachusetts Institute of Technology (MIT) trying to find new antibiotics using AI to analyse chemical compounds (Trafton 2020).

Admittedly, there are cases in which we do need personal data—medicine being a prime example. While medicine justifies collecting some personal data (e.g. clinical tests, a list of symptoms, etc.), it doesn't justify having the ubiquitous surveillance and trade in personal data that we currently have. Arguing that ubiquitous surveillance is unnecessary and disproportionate doesn't amount to arguing that we can never use personal data. Collecting data in medical contexts is perfectly justified. Selling that data and collecting personal data everywhere might not be.

A final response is that it is uncertain whether the AI of the future will need as much data as it does today. Part of what it means to be intelligent is the ability to generalize knowledge from a limited number of examples, like human beings do. A child doesn't need hundreds of thousands of images of dogs to recognize dogs. As AI systems become smarter, we can expect them to need less data (Wilson et al. 2019; Marcus and Davis 2020). The most important challenges to the development of AI are technical ones, and they won't necessarily be solved by collecting more data (Schneier and Waldo 2019).

Here again, if the ubiquitous surveillance facilitated by the trade in personal data is not necessary for technological advancement, it can hardly be proportionate, and it is far from clear whether it is necessary to

collect as much personal data as possible. The burden of proof is on those who claim it is.

Surveillance, freedom, and democracy

For decades, thinkers have worried about the negative consequences of surveillance for society, freedom, and liberal democracy. Ruth Gavison, for example, argued that:

> In the absence of consensus concerning many limitations of liberty, and in view of the limits on our capacity to encourage tolerance and acceptance and to overcome prejudice, privacy must be part of our commitment to individual freedom. [...] Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy.
>
> (Gavison 1980: 455)

In a similar vein, Thomas Nagel argued that, for the public sphere to be 'comfortably habitable' for different kinds of people, we need 'a culture that is publicly reticent'. For liberal democracy to work well, there must be a concomitant 'cultural liberalism' in which citizens allow each other to have enough privacy, which is essential to protect individual freedom and to avoid unnecessary conflicts in the public sphere (Nagel 1998).

Boudewijn de Bruin has argued that invasions of privacy can decrease people's negative freedom, which implies that privacy is a liberal value (de Bruin 2010). When companies and governments treat us differently as a result of privacy invasions, the opportunities we are afforded in life are being affected. If we end up self-censoring in an effort to better our life chances, our freedom is diminished even more. The losses of freedom due to self-censorship and external pressures to comply with algorithmic expectations can then lead to conformity.

Ubiquitous surveillance endangers fundamental personal, civic, and professional relationships. It can undermine intimacy between friends and family, freedom of association between citizens, and attorney–client privilege, among other things. Surveillance jeopardizes fundamental democratic practices like the secret ballot (Lever 2015) and investigative journalism.

It may not be a coincidence that Mexico, the deadliest country in the world for journalism in 2020, accounting for almost one-third of journalists killed that year worldwide (Lakhani 2020), was revealed to also be a hotspot for spying on journalists and human rights activists (Sheridan 2021). The Pegasus Project was an investigation which revealed that more than 50,000 journalists, human rights workers, academics, and other notable figures were being spied on by governments around the world. More than 15,000 of the victims were Mexicans—the most represented nationality on the list (Schwartz 2021). When journalists don't have enough privacy, they can't keep either themselves or their sources safe, which leads to the deterioration of the practice of journalism. Sources don't dare approach journalists, and journalists don't dare approach dangerous investigations. In turn, when journalism deteriorates, so does democracy as democracy depends on a well-informed citizenry.

Other related concerns regarding surveillance and society include the undermining of the presumption of innocence by treating all citizens as potential suspects (Hadjimatheou 2017), asymmetries of knowledge that tend to lead to asymmetries of power (Véliz 2020), and the risk of a massive misuse of personal data, for example, for the purposes of genocide. In the past, personal data has been grossly misused, as when Nazis raided local registries in search of data about Jewish people (Seltzer and Anderson 2001), and the best predictor that something can happen in the future is if it has happened in the past.

Conclusion: The danger of the surveillance delusion

Given the risks, harms, and wrongs of the kind of ubiquitous surveillance that has become common in the digital age, the burden of proof seems to be with defenders of the practice. There is at least one important challenge in that debate, however.

What is common to the risks, harms, and wrongs of surveillance is that they are difficult to quantify. It is easier to calculate the possible benefits of surveillance in terms of security, economic gain, and scientific

advancement than it is to put a price on our losses. We can easily put a price tag on how much we can hope to earn per year, say, through personalized ads. But how do we assess to what extent investigative journalism can be undermined by surveillance? And if journalism is not a particularly profitable endeavour, how do we assess its value for democracy? How do we evaluate the loss to society entailed by people self-censoring themselves in their daily life? As a result of these unanswered questions, I suspect we are prone to end up buying into what I call the *surveillance delusion*: the assumption that surveillance has no significant moral costs.

In *The Tyranny of Metrics,* Jerry Z. Muller warns against an obsession with metrics. Metric fixation 'may draw effort away from the things we really care about' and 'almost inevitably leads to a valuation of short-term goals over long-term purposes', he writes (Muller 2018: 3, 20). The flourishing of a kind of AI that heavily depends on data has further encouraged an obsession with metrics. But there are certain valuable things (e.g. intimacy, autonomy, freedom, and democracy) that are harder to quantify than others (e.g. economic gain through the trade in personal data) but no less valuable.

Not only are many of the downsides of surveillance hard to quantify, but the consequences of surveillance are also often delayed, which further feeds into the surveillance delusion. Even in relatively simple cases, it might be years until a data leak is felt. Sensitive data can spend years in the dark web before a criminal makes use of it. That delay makes it hard to make the connection between the loss of a particular data point and a concrete negative consequence. The connection in the realm of societal harms is even more delayed and harder to establish. Journalism may survive for a few years or maybe even decades without privacy, and its erosion may be so gradual as to be hard to perceive. A faded kind of democracy may withstand some disproportionate surveillance for some years too.

What is dangerous about the surveillance delusion is that it pushes us to appreciate the possible benefits of surveillance without taking seriously its possible costs. Given the close relationship between authoritarian regimes and the aspiration for ubiquitous surveillance, evidenced in historical examples from the East German Stasi to contemporary China, the surveillance delusion can end up having a very high price even if it cannot be monetized until it's too late.

An urgent question, then, is how much surveillance is too much to sustain liberal democracy, freedom, and the ways of life that we value? David Omand suggests that 'one defining difference between the practice of domestic intelligence collection in liberal democratic states and that in totalitarian states is the *extent* of it' (Omand and Phythian 2018: 36). On that account, our society does not seem to be faring well, even in comparison with a society like East Germany. We are collecting more personal data than ever before. If Katerina Hadjimatheou is right that intrusiveness is determined by reasonable expectations, the ability to plan for and consent to surveillance, the number of people given access to sensitive information, the sensitivity of the data, and the period for which data is retained (Hadjimatheou 2014: 196), it again looks like our societies are the most intrusive ones that have ever existed.

What a reflection on the surveillance delusion suggests is that, to answer the question of how much surveillance is too much, we need to go beyond short-term concerns and think about the kind of society we want to have decades from now. We need to think carefully about the requirements of autonomy, freedom, equality, and democracy to make sure that surveillance is not creating graver problems in the long run than the ones it is purporting to solve.

References

Allen, Anita (1988), *Uneasy Access: Privacy for Women in a Free Society* (Washington, DC: Rowan and Littlefield).
Google Scholar Google Preview WorldCat COPAC

Alvaredo, Facundo, Chancel, Lucas, Piketty, Thomas, Saez, Emmanuel, and Zucman, Gabriel (2018), *World Inequality Report 2018* (World Inequality Lab, The World Wide Web).
Google Scholar Google Preview WorldCat COPAC

Anderson, David (2016), *Report of the Bulk Powers Review* (London: Her Majesty's Government).
Google Scholar Google Preview WorldCat COPAC

Andreotta, Adam J., Kirkham, Nin, and Rizzi, Marco (2021), 'AI, Big Data, and the Future of Consent', *AI & Society*. https://doi.org/10.1007/s00146-021-01262-5.

Beardsley, Elizabeth (1971), 'Privacy: Autonomy and Self-Disclosure', in J. Rowland Pennock and J.W. Chapman, eds, *Privacy: Nomos XIII* (New York: Atherton Press), 56–70.
Google Scholar Google Preview WorldCat COPAC

Bergen, Peter, Sterman, David, Schneider, Emily, and Cahall, Bailey (2014), *Do NSA's Bulk Surveillance Programs Stop Terrorists?* https://www.jstor.org/stable/resrep10476#metadata_info_tab_contents.
WorldCat

Bezanson, Randall P. (1992), 'The Right to Privacy Revisited: Privacy, News, and Social Change, 1890–1990', *California Law Review* 80, 1133–1175.
Google Scholar WorldCat

Bidel, Susan, Parrish, Melissa, Verblow, Brandon, Egelman, Wei-Ming, and Turley, Christine (2017), 'Poor Quality Ads Cost US Marketers $7.4 Billion in 2016', in Forrester.

Brandl, Robert (2021), 'The World's Most Surveilled Citizens', *WebsiteToolTester*, https://www.forrester.com/report/Poor-Quality-Ads-Cost-US-Marketers-74-Billion-In-2016/RES136115.

Brown, Ian, and Korff, Douwe (2009), 'Terrorism and Proportionality of Internet Surveillance', *European Journal of Criminology* 6, 119–134.
Google Scholar WorldCat

Cameron, Joel D. (2021), 'Stasi', in *Encyclopedia Britannica*. https://www.britannica.com/topic/Stasi.

Carlile, Jennifer (2004), 'In Britain, Somebody's Watching You', *NBC News*, 9 Sept.

Clarke, Richard A., Morell, Michael J., Stone, Geoffrey R., Sunstein, Cass R., and Swire, Peter (2013), 'Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies'. https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world.
WorldCat

Cox, Joseph (2020), 'CBP Refuses to Tell Congress How It is Tracking Americans without a Warrant', *Vice*, 23 October.

Crawford, Kate (2021), *Atlas of AI* (New Haven, CT: Yale University Press).
Google Scholar Google Preview WorldCat COPAC

Cuters, Bart (2016), 'Click Here to Consent Forever: Expiry Dates for Informed Consent', *Big Data & Society* 1, 1–6.
Google Scholar WorldCat

de Bruin, Boudewijn (2010), 'The Liberal Value of Privacy', *Law and Philosophy* 29, 505–534.
Google Scholar WorldCat

Edelman, Gilard (2020), 'Ad Tech Could Be the Next Internet Bubble', *Wired*, 5 October.

Fabre, Cécile (2022), *Spying through a Glass Darkly. The Ethics of Espionage and Counterintelligence* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Fried, Charles (1970), *An Anatomy of Values* (Cambridge, MA: Harvard University Press).
Google Scholar Google Preview WorldCat COPAC

Garrett, Roland (1974), 'The Nature of Privacy', *Philosophy Today* 89, 421–472.
Google Scholar WorldCat

Garton Ash, Timothy (1997), *The File. A Personal History* (New York: Vintage Books).
Google Scholar Google Preview WorldCat COPAC

Gavison, Ruth (1980), 'Privacy and the Limits of Law', *Yale Law Journal* 89, 421–471.
Google Scholar WorldCat

Gerstein, Robert (1978), 'Intimacy and Privacy', *Ethics* 89, 86–91.
Google Scholar WorldCat

Gross, Hyman (1971), 'Privacy and Autonomy', in J. Rowland. Pennock and John W. Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press), 375–385.
Google Scholar Google Preview WorldCat COPAC

Hadjimatheou, Katerina (2014), 'The Relative Moral Risks of Untargeted and Targeted Surveillance', *Ethical Theory and Moral Practice* 17, 187–207.
Google Scholar WorldCat

Hadjimatheou, Katerina (2017), 'Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence', *Philosophy and Technology* 30, 39–54.
Google Scholar WorldCat

Helm, Toby (2019), 'Patient Data from GP Surgeries Sold to US Companies', *Observer*, 7 December.

Hill, Kashmir (2021), 'A Fire in Minnesota. An Arrest in Mexico. Cameras Everywhere', *New York Times*, 28 September.

Hwang, Tim (2020), *Subprime Attention Crisis* (New York: Farrar, Straus and Giroux).
Google Scholar Google Preview WorldCat COPAC

ICO (2019), *Update Report Into Adtech and Real Time Bidding* (London: Information Commissioner's Office).
Google Scholar Google Preview WorldCat COPAC

Isikoff, Michael (2013), 'NSA Program Stopped No Terror Attacks, Says White House Panel Member', *NBC News*, 20 December.

Jonas, Jeff, and Harper, Jim (2006), 'Effective Counterterrorism and the Limited Role of Predictive Data Mining', *Cato Institute, Policy Analysis*, 584.
Google Scholar WorldCat

Koehler, John O. (1999), *Stasi: The Untold Story of the East German Secret Police* (Boulder, CO: Westview Press).
Google Scholar Google Preview WorldCat COPAC

Kosinski, Michal, Stillwell, David, and Graepel, Thore (2013), 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior', *Proceedings of the National Academy of Sciences of the United States of America* 110, 5802–5805.
Google Scholar WorldCat

Lakhani, Nina (2020), 'Mexico World's Deadliest Country for Journalists, New Report Finds', *The Guardian*, 22 December.

Lever, Annabelle (2015), 'Privacy and Democracy: What the Secret Ballot Reveals', *Law, Culture and the Humanities* 11, 164–183.
Google Scholar WorldCat

Levin, Sam (2018), 'Tech Firms Make Millions from Trump's Anti-Immigrant Agenda, Report Finds', *The Guardian*, 23 October.

Levy, Steven (2014) 'I Spent Two Hours Talking with the NSA's Bigwigs. Here's What Has Them Mad', *Wired*, 13 January.

Macnish, Kevin (2015), 'An Eye for an Eye: Proportionality and Surveillance', *Ethical Theory and Moral Practice* 18, 529–548.
Google Scholar WorldCat

Macnish, Kevin (2016), 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World', *Journal of Applied*

Philosophy 35(2), 417–432.
Google Scholar WorldCat

Marcus, Gary, and Davis, Ernest (2020), *Rebooting AI. Building Artificial Intelligence We Can Trust* (New York: Vintage).
Google Scholar Google Preview WorldCat COPAC

Marmor, Andrei (2015), 'What is the Right to Privacy?', *Philosophy and Public Affairs* 43, 3–26.
Google Scholar WorldCat

Marr, Bernard (2018), 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read', *Forbes*, 21 May.

McMahan, Jeff (2009), *Killing in War* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Melendez, Steven, and Pasternack, Alex (2019), 'Here Are the Data Brokers Quietly Buying and Selling Your Personal Information', *Fast Company*, 2 March.

Morrison, Sara (2021), 'Here's How Police Can Get Your Data—Even If You Aren't Suspected of a Crime', *Vox*, 31 July.

Muller, Jerry Z. (2018), *The Tyranny of Metrics* (Princeton, NJ: Princeton University Press).
Google Scholar Google Preview WorldCat COPAC

Nagel, Thomas (1998), 'Concealment and Exposure', *Philosophy and Public Affairs* 27, 3–30.
Google Scholar WorldCat

Ng, Alfred (2020), 'Google is Giving Data to Police Based on Search Keywords, Court Docs Show', *CNET*, 8 October.

Nissenbaum, Helen (2010), *Privacy in Context. Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press).
Google Scholar Google Preview WorldCat COPAC

Omand, David, and Phythian, Mark (2018), *Principled Spying* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Parent, William A. (1983), 'Recent Work on the Concept of Privacy', *American Philosophical Quarterly* 20, 341–355.
Google Scholar WorldCat

Parker, Richard (1974), 'A Definition of Privacy', *Rutgers Law Review* 27, 275–297.
Google Scholar WorldCat

Rachels, James (1975), 'Why Privacy is Important', *Philosophy and Public Affairs* 4, 323–333.
Google Scholar WorldCat

Reiman, Jeffrey (1976), 'Privacy, Intimacy and Personhood', *Philosophy and Public Affairs* 6, 26–44.
Google Scholar WorldCat

(2009), 'Report on the President's Surveillance Program'. Washington DC.

Rumbold, Benedict, and Wilson, James (2019), 'Privacy Rights and Public Information', *Journal of Political Philosophy* 27, 3–25.
Google Scholar WorldCat

Savage, Charlie (2015a), 'Declassified Report Shows Doubts about Value of N.S.A.'s Warrantless Spying', *New York Times*, 25 April.

Savage, Charlie (2015b), *Power Wars. Inside Obama's Post-9/11 Presidency* (New York: Little, Brown and Company).
Google Scholar Google Preview WorldCat COPAC

Schneier, Bruce (2015), *Data and Goliath* (London: Norton).
Google Scholar Google Preview WorldCat COPAC

Schneier, Bruce (2018), *Click Here to Kill Everybody. Security and Survival in a Hyper-Connected World* (New York: W.W. Norton & Company).
Google Scholar Google Preview WorldCat COPAC

Schneier, Bruce, and Waldo, James (2019), 'AI Can Thrive in Open Societies', *Foreign Policy*, 13 June.

Schwartz, Leo (2021), 'Mexico's Shockingly Broad Use of Spyware is a Revelation. Nothing Will Change', *Washington Post*, 28 July.

Seltzer, William, and Anderson, Margo (2001), 'The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses', *Social Research* 68, 481–513.
Google Scholar WorldCat

Sheridan, Mary Beth (2021), 'How Mexico's Traditional Political Espionage Went High-Tech', *Washington Post*, 21 July.

Singel, Ryan (2009), 'Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims', *Wired*, 17 December.

Solove, Daniel J. (2001), 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review* 53, 1393–1462.
Google Scholar WorldCat

Solove, Daniel J. (2011), *Nothing to Hide* (New Haven: Yale University Press).
Google Scholar Google Preview WorldCat COPAC

Statista (2020), 'Worldwide Data Creation', https://www.statista.com/statistics/871513/worldwide-data-created, accessed 6 September 2022.
WorldCat

Thompson, Stuart A., and Warzel, Charlie (2019), 'How to Track President Trump', *New York Times*, 20 December.

Trafton, Anne (2020), 'Artificial Intelligence Yields New Antibiotic', *MIT News Office*, 20 February.

Véliz, Carissa (2017), *On Privacy* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Véliz, Carissa (2019), 'Medical Privacy and Big Data: A Further Reason in Favour of Public Universal Healthcare', in Andelka Phillips, ed., *Philosophical Foundations of Medical Law* (Oxford: Oxford University Press), 306–319.
Google Scholar Google Preview WorldCat COPAC

Véliz, Carissa (2020), *Privacy is Power* (London: Bantam Press).
Google Scholar Google Preview WorldCat COPAC

Véliz, Carissa (2021), 'Self-Presentation and Privacy Online', *Journal of Practical Ethics* 7(2), 30–43.
Google Scholar WorldCat

Véliz, Carissa (forthcoming), *The Ethics of Privacy and Surveillance* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Wasserstrom, Richard (1978), 'Privacy: Some Arguments and Assumptions', in Richard Bronaugh, ed., *Philosophical Law* (Westport, CT: Greenwood Press), 317–332.
Google Scholar Google Preview WorldCat COPAC

Westin, Alan F. (1970), *Privacy and Freedom* (London: Bodley Head).
Google Scholar Google Preview WorldCat COPAC

Wilson, James H., Daugherty, Paul R., and Davenport, Chase (2019), 'The Future of AI Will Be about Less Data, Not More', *Harvard Business Review*, https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more, accessed 14 January 2019.

Wooldridge, Michael (2020), *The Road to Conscious Machines: The Story of AI* (London: Pelican Books).
Google Scholar Google Preview WorldCat COPAC

Wright, Lawrence (2008), 'The Spymaster', *The New Yorker*, 21 January.

Wylie, Christopher (2019), *Mindf*ck. Inside Cambridge Analytica's Plot to Break the World* (London: Profile).
Google Scholar Google Preview WorldCat COPAC

Yadron, Danny (2016), '"Worth It": FBI Admits It Paid $1.3 to Hack into San Bernardino iPhone', *The Guardian*, 21 April.

Notes

1 Bernard Marr estimated in 2018 that 90 per cent of the data in the world had been generated in the previous two years (Marr 2018). According to Statista, data creation has continued its steady growth in the past few years (Statista 2020).

2 For more on the ethics of inferring sensitive information from public information, see Rumbold and Wilson (2019). For more on the ethics of taking personal information outside of the context it was given in, see Helen Nissenbaum's theory of contextual integrity (Nissenbaum 2010).

3 While some countries tend to define harm in utilitarian terms (e.g. psychological, physical, financial, reputational, etc.), other countries tend to focus on rights violations. On both frameworks, however, it is thought that consent can make an otherwise unethical case of data collection ethical (as exemplified by the General Data Protection Regulation in Europe and the California Consumer Privacy Act in the United States).

4 For more on the challenges of consent in the context of big data, see Cuters (2016), Andreotta et al. (2021), and Véliz (2019).

5 Control theories of privacy include Fried (1970), Bezanson (1992), Parker (1974), Beardsley (1971), Gerstein (1978), Rachels (1975), Reiman (1976), Marmor (2015), Wasserstrom (1978), and Westin (1970).

6 Access-based theories of privacy include Allen (1988), Garrett (1974), Gavison (1980), Gross (1971), and Parent (1983).

7 For an authoritative account of this unfolding, see Wooldridge (2020).