BOOK REVIEW

Privacy is Power: Why and How you Should Take Back Control of Your Data by Carissa Véliz (2020) Bantam, London, 288pp., £15 (hardback) ISBN: 9781787634046

Privacy at the Margins by Scott Skinner-Thompson (2020) Cambridge University Press, Cambridge, 220pp., £25 (paperback) ISBN: 9781316632635

We all know that 2020 was in many ways a terrifying year. Not only did we have to live through a pandemic, we also remember the violent ways that Black Lives Matter protesters were quelled. Those working in privacy law or ethics will probably remember 2020 as the year that a new infrastructure was developed: the contact tracing apps. Others, engaged in civil rights, will remember the surveillance of Black Lives Matter members in the US. Two recent books, published within a month of each other in September and October 2020, engage with both types of surveillance. Carissa Véliz uncovers in *Privacy is Power* how our data are used by high-technology companies and governments, and treats in more detail why we should be wary of contact tracing apps. On the other hand, Scott Skinner-Thompson examines how the privacy of marginalized communities (such as black, gay, trans and religious communities) is often violated and proposes a new way of understanding privacy.

Privacy is Power

In *Privacy is Power*, Carissa Véliz describes how tech companies and governments harvest your data, track you through everything you do, capitalize on that and thus endanger your privacy. Véliz, from the institute for ethics in AI at Oxford, has written a highly accessible book that not only warns of the dangers present in surveillance capitalism, but also explains why we should care about privacy and how we can increase it.

Véliz shows through six chapters and many examples how privacy is invaded – even in ways not normally noticed. After an introduction of the many ways data are harvested during a normal workday, Véliz goes into more detail of how this became business as usual. She finds it in the attacks of 9/11 and the subsequent focus on security, the discovery that personal data could be turned into profit (as shown by pioneer Google) and the belief that privacy is an outdated value. Combining these three has resulted in a surveillance capitalist world in which everyone surrenders privacy.

Véliz discusses what privacy is good for – namely protecting autonomy – and thus how it protects against the power of technologies. Building on Rainer Forst, she identifies, on the one hand, hard power, the power that forces you to act in a certain way (say, the fact that Google stores location data even when location history is turned off). On the other hand, there is soft power, the less forceful yet manipulative type of power (think of Twitter making you scroll down your feed every minute). Véliz argues that these types of power in the surveillance economy violate our privacy. Privacy is necessary for autonomy as it provides time and space to make decisions based on personal convictions. A violation of privacy curtails autonomy, the ability and right to govern oneself. Moreover, Véliz argues, interference with our autonomy is not just an infringement of personal liberty: democracy depends on others also being autonomous.

Privacy also has a collective dimension. DNA test results never apply to just one person, but always to their relatives as well. For example, if insurance companies ask higher premiums because

we might be susceptible to some inherited disease, others will experience these harms as well. One other way in which this is experienced is when people are manipulated through personalized fake news, as with the Cambridge Analytica scandal: personalization removes the common ground among us, the common reality. This is exactly why privacy is necessary for democracy: having privacy gives us time and space to vote, to protest, to associate, to exercise our collective power as a polity. Moreover, Véliz argues, privacy functions as a blindfold to justice, so that everyone is treated equally and impartially.

The data economy is dangerous not just because it creates power imbalances, but also because it trades in toxic personal data. According to Véliz, personal data are toxic because they are sensitive, susceptible to misuse, hard to keep safe and desired by many. The mismanagement of such data can jeopardize national security, corrupt democracy, threaten liberal societies and endanger the safety of individuals. Bold statements, yet the attack on the Capitol building in Washington shows us all that that (personalized) fake news fractures the public sphere and our common ground. Privacy would protect us by giving us space, without manipulation. In the last two chapters, readers are given policy advice and personal tips. These range from stopping personalized advertising and the trade in personal data to refusing to accept cookies, choosing privacy wherever possible. The smarter the device, the more it is to be avoided.

Conception of privacy and autonomy

If there is such a thing as an ethics page-turner, this is surely one. It provides an excellent introduction for those unacquainted with the ethics of personal data and privacy or looking for policy advice on how to prevent and mitigate (informational) privacy harms. Even so, I feel the relationship between privacy and autonomy could have been developed in more detail as it is the backbone of the book. At times, the book alludes to how privacy is important for developing relationships: for example, to have intimate conversations or to have debates where one can be frank. Yet, the fact that autonomy and privacy are relational is neglected; privacy is treated as individual and collective.

To understand autonomy and privacy as relational, we need to first to broaden our idea of autonomy from 'the ability and right to govern yourself' (p.71) to the notion that we require social conditions to develop our autonomy. In other words, social context is critical (Christman, 2020). The difference between collective and relational privacy is important in precisely this way. As Véliz says, privacy enables autonomy and is thus a condition for living an autonomous life, but it is also relevant that privacy posits norms on how to govern interactions within social contexts (Steeves 2009; Nissenbaum 2010; Lanzing 2019). In this way, privacy not only provides room for decision-making, but it also enables people to control what they disclose to others. In other words, privacy norms foster and develop relations – between me and my doctor, between me and my colleagues, between me and my supervisor, my friends, my family. All these different relationships have different norms: I would disclose pretty intimate things to my doctor that I would not disclose to my colleagues, for example. If technological innovations interfere with our privacy, they interfere with the different privacy norms and thus how we present ourselves to others. For example, if you tell your GP that you are pregnant, you would expect the GP to keep this information confidential. Yet, if you tell the pregnancy tracker Ovia, this information might well end up with your employer (Harwell, 2019), which is not a great idea, to put it mildly, when pregnancy discrimination is rampant. Distinguishing between those relational norms would have deepened the analysis in *Privacy is Power*, because it would have shown in greater detail the harm that is done.

The same goes for the distinction between informational and decisional privacy. While the book doesn't strictly distinguish between the two, many examples do refer to them. Informational privacy is the right to have control over your information, while decisional privacy is the right to defend against interference with your decisions and actions. Often, the two interact and reinforce each other (Lanzing, 2018). Conceptualizing privacy in these terms shows how personalized fake

news interferes with our privacy, first by collecting and analysing personal information, then by manipulating us. Conceptual demarcation would suggest how to mitigate those specific harms.

A critical perspective

Even though the book does not explicitly conceptualize privacy and autonomy in this elaborate manner, it still gives a convincing account of the power of privacy. In particular, Véliz highlights the relationship between privacy, autonomy and democracy and shows us why we should value privacy as citizens. And, by providing many suggestions for policy makers, Véliz imagines a future where innovation (for example, in the medical sector) is possible without using (as much) personal data. Yet, one wonders whether such policy advice is feasible within a surveillance capitalist society. Put another way, does retracing our steps not require a true overhaul of the system?

Answering such a question requires going back to the notions of hard and soft power. Véliz borrows these concepts from Rainer Forst (2017), a philosopher who put forward a critical and relational theory of justice. Forst goes beyond the distinction between hard and soft power to elaborate on the concepts of domination and oppression that are the core of injustice. Domination and oppression are not explicitly mentioned in *Privacy is Power*, though one case is studied extensively: during World War II, Jewish people in the Netherlands were killed at a far higher rate than Jews in other European countries. One explanation is that the Netherlands collected a lot of population data, including religion, and had mechanisms to record and process the data. In other words, privacy provides protection not only for the individual, but also for groups that are structurally oppressed in society.

Véliz suggests that privacy functions as a blindfold to justice. This is only true if privacy is applied equally, but we know that privacy is not applied equally to all. Those who are poor or marginalized often lose out. Routinely, the poor – which is often a proxy for race – do not have a right to privacy as their data are gathered in a multitude of ways and as they are made visible to both the state and companies. If homeless people apply for social housing in Los Angeles, they must first go through the maze of the digital coordinated entry tool (Eubanks, 2018). If they apply for state-funded pregnancy aid, poor women have to reveal the most intimate details of their life (Bridges, 2017). In other words, the privacy of marginalized people is even more endangered than that of other people. New technologies exacerbate inequalities and amplify racism (Benjamin, 2019). While Véliz does an excellent job of explaining how dangerous the surveillance economy can be, and acknowledges that technologies perpetuate sexism and racism (p.60), the general analysis would have benefited from a more fundamental theorization, which in turn would have had implications for policy making.

Privacy at the Margins

It is precisely here where Scott Skinner-Thompson's *Privacy at the Margins* is most relevant. Skinner-Thompson, from the University of Colorado Law School, draws on his law review papers and thus his book is aimed at a somewhat different audience. It would help to be familiar with US constitutional law or US civil rights law. However, readers with a background in privacy (law) are probably not unfamiliar with this discourse. Besides law, Skinner-Thompson also engages with the literatures of surveillance studies, critical data studies and critical theory. The book's six chapters are detailed and dense.

Skinner-Thompson offers a rich and powerful account of how we should understand privacy within US doctrinal law. The right to privacy is often sacrificed in courts. Skinner-Thompson shows how privacy can be beneficial to marginalized groups in society – if properly theorized and understood. He details how the privacy of marginalized people is disproportionately violated, and analyses how legal theories of privacy have given inadequate attention to the importance of privacy to marginalized communities and failed to account for the particular material harms they incur when their privacy is violated. He then proposes new ways of thinking about privacy, so, that the right to privacy would provide a suitable line of reasoning in court.

In the US under the secrecy paradigm (where privacy is consigned to the private sphere), privacy is severely limited in public. For example, the third-party doctrine holds that once information has been voluntarily given to third parties, you can no longer reasonably expect to have privacy with regard to that information. As Skinner-Thompson explains, this means that minorities can be severely disadvantaged; for example, when someone shares information within a certain context and then is no longer entitled to legal protection. This is exacerbated once more data are gathered (by state and companies alike) and thus become public. Skinner-Thompson proposes thinking of privacy as serving both an anti-subordination and an expressive goal. Conceptualizing privacy in this way would provide a proper defense against interferences.

The expressive goal of privacy is exemplified by the person who wears a hoodie or mask to shield their identity and body. This person might be engaged in a form of expressive resistance to the surveillance regime – and in that way 'performs' privacy. Performative privacy draws out the invisible (state) power structures and exposes surveillance. At the same time, performative privacy serves autonomy through the act of expression. In the same way, obfuscation technologies, such as TrackMeNot or Tor, protest against online surveillance. Privacy as a form of expression then may put privacy within the scope of free speech (the First Amendment in the US) and thus be provided with more protection. It would, for example, provide a rebuttal for companies like Clearview AI that rely on the First Amendment while at the same time scraping the internet for images to use in their facial recognition software. Viewing such acts as performative privacy also furthers anti-subordination goals. By resisting surveillance, people assert their existence within the public sphere and so reclaim that space. As anti-subordination has received the protection of the courts, this conception would increase privacy protection. Skinner-Thompson then argues that information disclosed by the state often threatens further subordination of marginalized groups or beliefs. He suggests that informational privacy should specifically protect intimate and political information as those types of information are more likely to result in material consequences, such as discrimination. Tangible harms would be protected by the courts: intangible harms to autonomy and dignity would not.

Protections and legal doctrine

The two strongest points of Skinner-Thompson's scholarship are 1) his notion of privacy being performative, both expressive and anti-subordinate; and 2) his compelling argument that marginalized communities encounter more surveillance (and thus have to share their information, and have less privacy protection) than more privileged groups that can either avoid surveillance or pay to keep their information secret. This is of importance to any concept of privacy and could guide legal doctrine well beyond the US.

Some arguments in the book are much more US-focused. Consider his argument that the courts should not be focused on autonomy violations as such, but should focus on more palpable harms, as when intimate or political categories of information are disclosed. Here I have some disagreement with Skinner-Thompson in that a lot of these harms would still entail an interference with either informational or decisional privacy or autonomy. It is not just the disclosure that constitutes a harm. For example, immigration and customs enforcement investigators in the US used a private database (updated daily) with hundreds of millions of utility records to track down people, raid their homes and deport them (Harwell, 2021). The government has no right to gather this data. It is an abuse of any right to information privacy and it interferes directly with people's autonomy as they can be deported at any moment. And yes, it also interferes with people's dignity as they have to choose between basic needs or the risk of deportation.

Perhaps our disagreement stems from the fact that US courts do not employ a clear privacy framework. That 'decisional privacy . . . seems to have bled into analysis regarding the role of informational privacy' (p.148) is a problem when the courts cannot employ a concrete framework to distinguish the two. In contrast, a much more concrete framework is provided in Europe through the European convention on human rights, the charter of the EU, and the general data protection

regulation. The last allows processing of sensitive data only as an exception. Envisaging tangible harms, such as Véliz describes in her book, can then be directly related to specific provisions.

Even if we do not disclose intimate or political information about ourselves as such, we may still reveal this information from other information; analysis of something as banal as Netflix records, for example (Narayanan and Shmatikov, 2007). Skinner-Thompson advocates robust privacy protection. Even so, can intimate and political information be truly protected if other personal data are not protected as well?

Concluding

Both books are excellent, though aimed at different audiences. Each has its own strengths and is highly topical, one referring to the pandemic and the other to the Black Lives Matter movement and protests. They complement each other: where *Privacy is Power* does a great job in providing a general overview in how surveillance capitalism violates our privacy, and thus endangers our autonomy and democracy, *Privacy at the Margins* focuses on marginalized communities and the unequal way in which privacy is applied. Where *Privacy is Power* highlights why we should value privacy from an ethical perspective and how we can pull the plug, *Privacy at the Margins* expands privacy protections from a legal point of view. One book focuses on data and technologies: the other shows that these have their counterpart in hoodies and veils.

Both books are relevant to the proposal to issue digital vaccination passports and to the consequent danger of creating an entire new surveillance infrastructure. We need *Privacy at the Margins* to analyse how such apps would endanger, for example, black communities. And we need it to open our minds to the idea that not using such an app could very well be an expressive act of resistance, which furthers anti-subordination. Yet, we need *Privacy is Power* to analyse how the surveillance infrastructures put in place by technology companies profit from our sensitive personal data. Mass surveillance does not make the world a safer place.

References

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*, Polity Press, Cambridge.

Bridges, K. (2017) *The Poverty of Privacy Rights*, Stanford University Press, Berkeley CA.

Christman, J, (2020) 'Autonomy in moral and political philosophy' in Zalta, E. (ed.) *The Stanford Encyclopedia of Philosophy*, available at https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/ (accessed March 2020).

Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, Picador, London.

Forst, R. (2017) *Normativity and Power*, Cambridge University Press, Cambridge.

Harwell, D. (2019) 'Who else is tracking your pregnancy?', *Washington Post*, 10 April.

Harwell, D. (2021) 'ICE investigators used a private utility database covering millions to pursue immigration violations', *Washington Post*, 26 February.

Lanzing, M. (2018) '"Strongly recommended": revisiting decisional privacy to judge hypernudging in self-tracking technologies', *Philosophy and Technology*, 31, 3, pp.549–68.

Lanzing, M. (2019) 'The transparent self: a normative investigation of changing selves and relationships in the age of the quantified self', PhD thesis, Department of Industrial Engineering and Innovation Sciences, Technische Universiteit Eindhoven.

Narayanan, A. and Shmatikov, V. (2008) 'Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset)', available at https://arxiv.org/pdf/cs/0610105.pdf (accessed March 2020).

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Berkeley CA.

Roessler, B. and Mokrosinska, D. (eds) (2015) *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge University Press, Cambridge.

Steeves, V. (2009) 'Reclaiming the social value of privacy' in Kerr, I., Steeves, V. and Lulock, C. (eds) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, Oxford, pp.191–208.

Jenneke Evers
Center for Law and Digital Technologies, Universiteit Leiden, Netherlands
g.h.evers@law.leidenuniv.nl