Privacy and digital ethics after the pandemic

The increasingly prominent — and inescapable — role of digital technologies during the coronavirus pandemic has been accompanied by concerning trends in privacy and digital ethics. But more robust protection of our rights in the digital realm is possible in the future.

Carissa Véliz

The coronavirus pandemic has permanently changed our relationship with technology, accelerating the drive towards digitization. While this change has brought advantages, such as increased opportunities to work from home and innovations in e-commerce, it has also been accompanied with steep drawbacks, which include an increase in inequality and undesirable power dynamics.

Power asymmetries in the digital age have been a worry since big tech became big. Technophiles have often argued that if users are unhappy about online services, they can always opt-out. But opting-out has not felt like a meaningful alternative for years for at least two reasons.

First, the cost of not using certain services can amount to a competitive disadvantage — from not seeing a job advert to not having access to useful tools being used by colleagues. When a platform becomes too dominant, asking people not to use it is like asking them to refrain from being full participants in society. Second, platforms such as Facebook and Google are unavoidable — no one who has an online life can realistically steer clear of them. Google ads and their trackers creep throughout much of the Internet[1], and Facebook has shadow profiles on netizens even when they have never had an account on the platform[2].

Citizens have responded to the countless data abuses in the past few years with what has been described as a 'techlash'[3]. Tech companies whose business model is based on surveillance ceased to be perceived as good guys in hoodies who offered services to make our lives better. They were instead data predators jeopardizing, not only users' privacy and security, but also democracy itself. During lockdown, communication apps became necessary for any and all social interaction beyond our homes. People have had to use online tools to work, get an education, receive medical attention, and enjoy much-needed entertainment. Gratefulness for having technology that allows us to stay in contact during such circumstances has thus watered down the general techlash. Big tech's stocks have been consistently on the rise during the pandemic, in line with its accumulating power.

As a result of the pandemic, however, any lingering illusion of voluntariness in the use of technology has disappeared. It is not only citizens who rely on big tech to perform their jobs: businesses, universities, health services, and governments need the platforms to carry out their everyday functions. All over the world, governmental and diplomatic meetings are being carried out on platforms such as Zoom and Teams. Since governments do not have full control over the platforms they use, confidentiality is uncertain.

Enhanced power asymmetries have also worsened the vulnerability of ordinary citizens in areas that range from the interaction with government to ordering food online, and almost everything in between. The pandemic has, for example, led to an increase in the surveillance of employees as they work from home[4]. Students are likewise being subjected to more scrutiny: by their schools and teachers, and above all, by the companies on which they depend[5]. Surveillance for public health purposes has likewise increased. Privacy losses disempower citizens and often lead to further abuses of power. In the UK, for example, companies collecting data for pubs and restaurants for contact-tracing purposes have sold on that information[6].

Such abuses are not isolated events. For the past two decades, we have allowed an unethical business model that depends on the systematic violation of the right to privacy to run amok. As long as we treat personal data as a commodity, there will be a high risk of it being misused — by being stolen in a hack or by being sold to the highest bidder (which often includes nefarious agents).

In addition to favouring digital technologies, power shifts resulting from the pandemic have also promoted authoritarian tendencies. Democracy is in retreat. According to Freedom House, a think-tank in Washington DC, democracy and respect for human rights have deteriorated

Credit: YAY Media AS / Alamy Stock Vector

in 80 countries since the outbreak of the coronavirus[7]. The pandemic has, in particular, greatly benefitted China and its approach to technology. By managing the pandemic much more successfully than Western countries, China has advanced years in its race against Western hegemony.

The task ahead

As the pandemic abates, the challenge will be to maintain the positive aspects that can come from an increase in digitalization, while minimizing the risks and harms, and attempting to recover any ground lost. This path is replete with possible pitfalls.

One concern is the increasing closeness between technology companies and governments. Tech billionaire and former Google CEO Eric Schmidt has, for instance, called for "unprecedented partnerships between government and industry"[8]. Palantir, the controversial Central Intelligence Agency (CIA)-backed company, is now collaborating with both the UK's National Health Service (NHS) and the

US Department of Health and Human Services[9]. The NHS, in particular, gave Palantir all kinds of data about patients, employees and members of the public — from contact information to details of gender, race, work, physical and mental health conditions, political and religious affiliation, and past criminal offences[10].

Prominent among the many privacy challenges citizens face in the wake of the pandemic are data deals that might consolidate widespread surveillance as a requirement to access primary services and opportunities. Given big tech's track record in violating people's privacy, its recent interest in expanding into the health sector is particularly alarming. Amazon's new Pharmacy promises 80% discounts, for example, which suggests that sensitive data may be of more interest to the retailer than immediate profits[11].

A related concern is that, in their effort to defeat China in the race towards the development of increasingly sophisticated artificial intelligence (AI), Western countries might continue to allow the trade in personal data, and may even be enticed to further liberalize personal data for the purposes of financial gain or competitive advantage[12]. Such an approach would be a mistake. True progress is not achieved by forsaking human rights. Beating China in a race to the moral bottom would not be a victory for the West. Instead, countries need to close ranks in defence of human rights. Diplomacy will be crucial in the coming years to meet the biggest challenges beyond the coronavirus pandemic, which include climate change and the regulation of digital technologies. Countries must try to come together and reach agreements on minimum standards and rules regarding cybersecurity, privacy and the governance of AI. If enough countries unite, they can make it attractive for China to cooperate.

Items on the agenda

Privacy needs to be a key item at the diplomatic negotiating table. Even the most capitalist societies do not allow certain kinds of trade that erode rights or valued ways of life. Personal data should not be something to be bought and sold. Duties of care should be attached to the collection and management of personal data. By collecting more personal data than we need, and by trading it for profit, we are creating our own risk as a society. Data misuse leads to inequality, mistrust, national security risks, and even to the erosion of democracy, as illustrated by the Cambridge Analytica scandal[13]. Trades in personal data should be banned, and fiduciary duties should be imposed on anyone who collects, manages or stores personal data[14].

Cybersecurity standards and rules are a second crucial item to reach agreements on. We need to build safer products. For that, we need to come up with international minimal standards and certifications, as well as pacts to ensure a relatively peaceful cyberspace that can be used safely by netizens and companies. Perhaps the most difficult and important challenge on the agenda will be to agree on AI ethical standards. Rules are needed to ensure accountability, fairness, safety, and the enhancement of individual autonomy.

Up until now, companies and governments have been using the general population as guinea pigs in their attempts to develop AI. Citizens are routinely subjected to algorithms that have not undergone a robust process of randomized controlled trials. On occasion, algorithms have never been used outside the lab, and we discover their faults once they have harmed someone. We do not allow that to happen with pharmaceutical drugs, and neither should we allow it to happen with algorithms that are involved in decisions that have a significant impact on people's lives.

Reasons for optimism

Despite the concerning trends regarding privacy and digital ethics during the pandemic, there are reasons to be cautiously optimistic about the future. First, citizens around the world are increasingly suspicious of tech companies, and are gradually demanding more from them. Second, there is a growing awareness that the lack of privacy ingrained in current apps entails a national security risk, which can motivate governments into action. Third, US President Joe Biden seems eager to collaborate with the international community, in contrast to his predecessor. Fourth, regulators in the US are seriously investigating how to curtail tech's power, as evidenced by the Department of Justice's antitrust lawsuit against Google and the Federal Trade Commission's (FTC) antitrust lawsuit against Facebook[15]. Amazon and YouTube have also been targeted by the FTC for a privacy investigation[16]. With discussions of a federal privacy law becoming more common in the US, it would not be surprising to see such a development in the next few years. Tech regulation in the US could have significant ripple effects elsewhere.

Societies have managed to regulate every significant industry that has ever existed — from railways, cars, and aviation to utilities, pharmaceuticals, and food. The task of our generation is to make sure that whatever rights we are owed offline are also respected online. Digital technologies can only constitute progress if they serve the well-being of citizens and the flourishing of democracy. ❐

Carissa Véliz ✉

Faculty of Philosophy and the Institute for Ethics in AI, University of Oxford, Oxford, UK.

✉*e-mail: carissa.veliz@philosophy.ox.ac.uk*

Published online: 25 January 2021
https://doi.org/10.1038/s41928-020-00536-y

References

1. Schofield, J. How can I remove Google from my life? *The Guardian* https://go.nature.com/3osHss6 (20 December 2018).
2. Brandom, R. Shadow profiles are the biggest flaw in Facebook's privacy defense. *The Verge* https://go.nature.com/3q1X9ak (11 April 2018).
3. The techlash against Amazon, Facebook and Google—and what they can do. *The Economist* https://go.nature.com/2K41ZAA (20 January 2018).
4. Satariano, A. How my boss monitors me while I work from home. *The New York Times* https://go.nature.com/3orMSns (6 May 2020).
5. Kshetri, N. Remote education is rife with threats to student privacy. *The Conversation* https://go.nature.com/3beQhCi (6 November 2020).
6. Das, S. & Mararike, S. Contact-tracing data harvested from pubs and restaurants being sold on. *The Times* https://go.nature.com/3osQq8L (11 October 2020).
7. Repucci, S. & Slipowitz, A. *Democracy Under Lockdown* https://go.nature.com/3olGn5v (Freedom House, October 2020).
8. Schmidt, E. Eric Schmidt: I used to run Google. Silicon Valley could lose to China. *The New York Times* https://go.nature.com/2Luj0Z5 (27 February 2020).
9. Morrison, S. Everything you need to know about Palantir, the secretive company coming for all your data. *Vox* https://go.nature.com/3q1C0Ny (26 August 2020).
10. Thomson, A. & Browning, J. Peter Thiel's Palantir is given access to U.K. health data on Covid-19 patients. *Bloomberg* https://go.nature.com/3hUTpV7 (5 June 2020).
11. Couldry, N. & Ali Mejias, U. Big Tech's latest moves raise health privacy fears. *Financial Times* https://go.nature.com/2MBIhkm (7 December 2020).
12. Véliz, C. You've heard of tax havens. After Brexit, the UK could become a 'data haven'. *The Guardian* https://go.nature.com/38pTvkE (17 October 2020).
13. Cambridge Analytica files. *The Guardian* https://go.nature.com/38r9rmy (2018).
14. Véliz, C. *Privacy Is Power* (Bantam Press, 2020).
15. Paul, K. 'This is big': US lawmakers take aim at once-untouchable big tech. *The Guardian* https://go.nature.com/38pgWKC (19 December 2020).
16. Kelly, M. The FTC is investigating data collection at YouTube, Facebook, and seven other companies. *The Verge* https://go.nature.com/3ompLdQ (14 December 2020).

Competing interests

The author declares no competing interests.