Privacy During the Pandemic and Beyond

Carissa Véliz on privacy challenges in a changed world

During the past two decades, privacy has been a fierce battle ground. At the beginning of the century, newly founded tech companies like Google started the fight by establishing a novel business model based on surveillance. Our personal data became the golden nuggets of the digital era. But it would be years before ordinary citizens realised the deal they had struck when they had "agreed" to indecipherable, extensive, and constantly changing terms of service. Once we realised the extent to which our data was being collected and analysed, it seemed like it was too late to recall it, and many public voices declared the death of privacy.

Recovering privacy seemed all the more impossible given governments' support of corporate surveillance. The data economy became a way to enhance the information capabilities of intelligence agencies, which were looking to increase their power after the trauma of the terrorist attacks on the Twin Towers in the United States in 2001. From the start, the surveillance economy has sprung from and been sustained by cooperation between corporations and governments.

Tech companies were only too happy to echo the discourse on the death of privacy. It was a narrative that was good for business. In 2010, Mark Zuckerberg suggested that privacy social norms had "evolved", that people were more comfortable sharing more, and that Facebook was merely reflecting the current social norms. The more people shared online, the more personal data tech companies could collect, the more they could personalise ads and content, the more they could influence users' behaviour, the more users engaged, the more ads they could sell.

Almost every week for the past few years, privacy has been a major news headline – data breach after data breach

Then came the privacy scandals. Almost every week for the past few years, privacy has been a major news headline. Data breach after data breach, cases of data collected without consent, legal and illegal data misuses. Users' passwords getting published, people being extorted, data brokers using people's most sensitive information (that they were rape victims, that they were impotent, that they were AIDS patients) to sell their profiles to the highest bidder. Perhaps the pinnacle of the privacy disasters saga was the

Cambridge Analytica data scandal, revealed in 2018. The British data firm had used the personal data of over 87 million users to build psychographic profiles of voters around the world in order to design personalised political propaganda and sway elections. Cambridge Analytica helped both the Trump presidential campaign in the United States and the Leave campaign in the Brexit referendum in the United Kingdom.

Citizens responded to the privacy scandals with what has been described as a "techlash". Tech companies whose business model depends on surveillance were no longer perceived as the good guys in hoodies who were here to make our world a better place. They were data predators that were jeopardising, not only individuals' privacy and security, but also democracy itself. Regulators turned their attention towards privacy, implementing the General Data Protection Regulation in Europe, the California Consumer Privacy Act, and discussing a possible federal law in the United States, among other regulatory initiatives. Privacy turned out to be far from dead.

Then came the pandemic.

Power shifts

The coronavirus pandemic has aggravated power asymmetries that were being challenged before the world went into lockdown. Before the pandemic, resistance was building against tech companies' hegemony. Against, for instance, terms of agreement that do not give users meaningful options and can change at any time. The pandemic, however, gave tech companies new leverage.

From the time tech companies like Facebook and Google became big tech, the option of not using them has been somewhat of a fiction. Tech enthusiasts have pointed out time and again that if users are unhappy about these services, they should simply opt-out of them. There are two main reasons why opting-out is not a meaningful alternative.

The pandemic has made technology even more pervasive

First, the cost of not using services that have become as necessary as utilities is inordinately high, both personally and professionally. Not using Facebook can mean losing hundreds of relationships, and missing out on crucial professional opportunities. Not using Google can amount to a competitive disadvantage -- from getting lost in an unfamiliar city on the way to a job interview, to not having access to research tools such as Google Scholar that are being used by one's colleagues. When a platform becomes as dominant as Facebook and Google are, asking someone not to use it amounts to asking them to exclude themselves from being full participants in their society.

Second, even if you try your best to avoid Facebook and Google, they're unavoidable. Google ads, and their trackers, for instance, are plastered throughout most of the internet. Facebook has a shadow profile on you even if you've never had an account with them. Your sacrifice ends up feeling useless.

Before the pandemic, however, there was more of an option to resist using tech services -- even if there was a high cost to pay, and even if one were still tracked by

them to a certain extent. During lockdown, that narrow possibility became even narrower, and any illusion of voluntariness in the use of technology has vanished.

For most people who have had to endure lockdown, the pandemic has made technology even more pervasive and inevitable. Being online and using videoconferencing apps became necessary for any and all social interaction beyond the walls of our homes. Key workers had to risk their lives by continuing to work outside their homes. Everyone else had to use online tools to get an education, work, interact with family, get medical attention, enjoy some much-needed entertainment, and more.

The choice between centralised and decentralised apps became the arena of the latest privacy feud

Thus, some of the techlash has been watered down by a combination of feeling grateful that we have technology that can allow us to stay in touch with others even while in lockdown, and resignation that boycotting tech seems less of an option than ever. Big tech's stocks have been consistently on the rise during the pandemic, in correlation with their accumulated power.

Dependence on smartphones and tech platforms is widespread. It's not only citizens depending on gadgets and apps to continue their studies or perform their jobs. Even businesses, universities, health services, and governments depend on these platforms to carry out their everyday functions. These institutions do not have platforms of their own. Government and diplomatic meetings around the world are being carried out on platforms such as Zoom and Teams. Universities cannot fully guarantee the privacy of their students because they do not control the platforms they use. Often, governments cannot be certain of the confidentiality of their meetings for the same reason.

There are, however, a few avenues of resistance and sources of friction that are proving crucial to protect privacy in these challenging times.

Avenues of resistance

Although resisting tech during lockdown is extremely hard, confinement could not last forever. There was an urgent economic need to resume more productive lifestyles as soon as possible. Once analogue life resumes its course, the possibilities for avoiding particular apps or technologies multiply.

Soon after lockdown began, governments around the world proposed a variety of contact-tracing apps as a possible solution to emerge from confinement in a safer way. Tech companies were quick to jump at the opportunity, offering their services to support this effort. But the distrust cultivated by years of misuses of data had taken its toll. Citizens, privacy experts, and concerned organisations sounded their alarms. Having learnt from the experience after 9/11, political commentators warned about "temporary" measures becoming entrenched. Enlisting experts' support was important because, unless governments were willing to try their luck at making the use of these apps mandatory -- risking

sabotage or rebellion from the population – they had to secure citizens' cooperation and trust. People have to download and use the app for it to work. Had governments and tech companies been more trustworthy with personal data in the past two decades, cooperation for the sake of public health could have been much more successful.

But experts had doubts about how useful such contact-tracing apps would be in the first place, given the difference between electronic "contacts" and infections. Apps allow for false positives, when two people seem to be in contact from the point of view of their phones but in fact are separated by a wall. Apps also invite false negatives, as they cannot record infections contracted from contaminated surfaces or from a contact between people who didn't have their phones on them, or who had too fleeting a contact to be recorded as such by the app. That apps were receiving so much attention – as opposed to efforts to produce more protective equipment, sanitising products, etc. – was questionable.

There were also doubts about how much data was necessary for an app to be useful. The United Kingdom's National Health Service, for instance, first championed a centralised approach according to which data would be sent to a centralised database from which networks of relationships and contacts could be gleaned. In contrast, decentralised apps are designed to process data in people's phones. Although the latter approach is less informative to health authorities (e.g. they cannot know who is suspected of infection, or who has been in contact with whom), it is much more protective of privacy, and equally effective at alerting people who might have been in contact with someone who has been diagnosed with Covid-19.

The choice between centralised and decentralised apps became the arena of the latest privacy feud. Apple and Google teamed up to build an API (application programming interface) to support decentralised contact-tracing apps, which meant that centralised apps were not going to work properly on iPhones and Androids. Given that the vast majority of people who have smartphones have one or the other brand, the UK was forced to change their approach to a decentralised app.

Privacy can sell

For citizens, the good news was that the tech giants protected their privacy better than might have been expected, given the track record of a company like Google. The bad news was that this power struggle made it obvious how big tech companies have more power than governments, and are often treated as if they were governments themselves. Tech users around the world are at the mercy of undemocratic and largely unaccountable corporations. It's great when they protect our privacy, but it's extremely bad news when they don't, and Google's business model still depends on personal data. That we have to trust the good will of giant corporations for our right to privacy to be respected is far from ideal.

The first avenue of resistance, then, came about as a result of the need to secure trust from the population in the post-lockdown world. One of the positive effects of the techlash before the pandemic hit was


© Sean Last

the proliferation of privacy-friendly (or friendlier) alternatives, which is the second resource for resistance. Privacy is something that can sell, an edge that can give a company competitive advantage. The more privacy the competition offers, the more other businesses are willing to cave to public pressures that call for more privacy.

End-to-end encryption, for instance, is slowly becoming an expected standard of cybersecurity. When it was revealed that Zoom did not offer end-to-end encryption despite claiming it did, the scandal led to the company promising such encryption. Zoom then announced it would only offer the added security to paid accounts. The public criticism quickly made the company commit to end-to-end encryption for all users.

Privacy-friendly tech empowers netizens first, by protecting their personal data; second, by providing meaningful options to dominant and privacy-unfriendly tech; and third, by pushing big tech towards offering more privacy protections to remain competitive.

But as long as big tech remains as dominant as it is today, privacy-friendly alternatives will not be able to compete on an equal footing on account of network effects (everyone wants to be in the most popular platform because that is where everyone else is), and decades of big tech having hoarded personal data (which helps platforms sell personalised ads and have more accurate algorithms), among other factors.

Challenges ahead

When tech companies and governments form a unified surveillance front, citizens are overpowered – they cannot count on governments to protect them from companies nor on companies to protect them from government surveillance. From that point of view, it is a good sign when there is disagreement between big tech and governments, as in the case of the debate between centralised and decentralised contact-tracing apps. The coronavirus pandemic, however, has brought new alliances between tech companies and governments that are concerning.

Our personal data should not be the kind of thing that can be bought, sold, or used against us

Tech billionaire and former Google CEO Eric Schmidt has argued for "unprecedented partnerships between government and industry". Palantir, the controversial CIA-backed company that collaborated in the United States' surveillance programme, is now involved with both the United Kingdom's National Health Service and the United States' Department of Health and Human Services, as well as the Centers for Disease Control and Prevention. The NHS 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. Palantir first charged the NHS just £1 for its services – in return, Palantir was granted intellectual property rights and access to valuable data to train their models. The company later secured a £1 million contract with the NHS for a coronavirus "data store".

Prominent among the many privacy

challenges citizens face in the wake of the pandemic, then, are corporate data deals with governments that might solidify widespread surveillance as a condition to access basic services and opportunities.

One of the things we lose when our privacy is jeopardised is autonomy – our ability to self-govern, both as individuals and as democracies. An important contribution of medical ethics was giving more autonomy to patients. As the deal between the NHS and Palantir shows (another infamous similar deal was between the NHS and DeepMind in 2016), patients' autonomy is being compromised by breaches in confidentiality. NHS patients are not being asked for the consent to transfer their data to corporations that are not health professionals and do not have patients' best interests as their main objective. The loss of autonomy in the medical context is happening in society more generally as a result of ubiquitous surveillance.

Privacy is important because the lack of it gives others power over us. If corporations and governments know who we are, what we fear, what we desire, whom we sleep next to, what motivates us, they can more easily influence our behaviour, as the Cambridge Analytica scandal illustrates. They can also discriminate against us – for our gender, race, genetic makeup, medical history, or ideas – without us ever knowing about it. And they can use our data to build tools that can later oppress us.

Companies such as Clearview AI, for example, have used the photographs that we have shared online to train their facial recognition algorithms, often without our knowledge or consent. Facial recognition, along with other technologies that strip away anonymity, is particularly dangerous to our privacy. At the time of writing, there are protests on both sides of the Atlantic over racial injustice. Can protestors be sure that they are protesting anonymously, given how common facial recognition has become? Can they be sure that participating (peacefully and legally) in a demonstration will not make them vulnerable to being targeted by the police? What about all the footage from our innumerable video calls? Can we be sure that facial recognition is not being used on those?

Our privacy should not be a bargaining chip. Our personal data should not be the kind of thing that can be bought, sold, or used against us by institutions that are supposed to be our data custodians. Institutions that violate people's privacy should face serious enough consequences that they regret having done so. There is a long way ahead of us in making governments and corporations accountable in matters of privacy. But that institutions found resistance to data grabs even during the worst of times, when we were a captive audience made vulnerable by the pandemic, gives us reason for optimism.

Carissa Véliz is an incoming associate professor in philosophy at the Institute for Ethics in AI at the University of Oxford and author of Privacy Is Power *(Bantam Press, 2020).*