Check for updates

## editorial

## Privacy debate obscures pandemic power shifts

Soon into the COVID-19 pandemic, civil-rights groups raised the alarm over the increase in digital surveillance infringing on individual rights. But there are other potential harms as tech companies accelerate their expansion into new areas essential to public-service provision.

he COVID-19 pandemic brought about a huge shift in how digital technology is used, both by citizens and by governments. As countries across the world locked down, governments and businesses scrambled for solutions to help their services adapt. Tech companies came with their answer, sometimes in the form of digital surveillance, such as software for keeping track of employees working from home. Business boomed for educational technology ('edutech'), including automated proctoring systems at universities.

A recent report by the Global Data Justice project, a European Research Councilfunded initiative to research the lived experience of data technologies worldwide, shows that this trend of expansion although accelerated by the pandemic has been a long-term aim for many private companies<sup>1</sup>. Businesses identified lucrative opportunities for partnering with public-service providers. For example, Palantir, a company known for its security and intelligence analytics, quickly offered its services to governments to monitor the spread of COVID-19. The development of native contact-tracing smartphone apps by Google and Apple solidified their budding interest in health-related technologies, to build upon their main revenue sources of advertising and hardware sales.

This type of sector creep, coined 'sphere transgression', occurs when digital expertise such as cloud computing gives companies a commercial advantage in other spheres such as health or education<sup>2</sup>. Taken on their own, many of these innovations are laudable, and have had a substantial impact on the course of the pandemic. But as private contractors become more enmeshed in the running of public services, a dependence on commercial digital infrastructures, from hardware to software, is created that is difficult to untangle.

User privacy emerged as a major concern about private-sector involvement early in the pandemic. Google and Apple, however, opted for a fully decentralized approach to contact-tracing apps that did not store location data, whereas many public-health services, such as those in the United Kingdom and Australia, initially attempted to also store users' location data. This flipped the script, with tech companies casting themselves as defenders of user privacy. The automated proctoring software Proctorio, for example, now touts its privacy-by-design approach and use of encryption as a selling point, after a court ruling that this software was compliant with the European Union's General Data Protection Regulation.

The focus on individual privacy and surveillance has subtly shifted the goalposts for what society finds acceptable. As long as technology is 'privacy-preserving', it would seem that it is safe to place it in classrooms, lecture halls and care homes. But the report by the Global Data Justice project notes that there are other forms of harm to consider when commercial digital technology is repurposed in other sectors — such as the potential for the disruption or genuine destabilization of mechanisms for providing public goods. During the pandemic, Google and Apple gained substantial influence in the domain of public health through their almost complete control over the operator systems that run on everyone's smartphones, but as the report states, they lack both epidemiological expertise and moral authority in this domain.

"I completely agree with the report that we need to think beyond the narrow focus on privacy or even data protection," Tamar Sharon of Radboud University told *Nature Machine Intelligence.* "The expansion of Big Tech into public sectors may reshape the health or education sectors in line with the values, norms and aims of these actors, which may clash with the traditional values, norms and aims of a sector."

A potential route to rein in the expansion of tech companies is via the European Union's upcoming Digital Markets Act and Digital Service Act, which would tackle the outsized influence of digital service providers. However, Sharon points out that thinking about sectors such as health, education and the media as markets might not be entirely appropriate. "They are not here to distribute market goods, but to provide essential public goods and to satisfy basic needs. Sphere transgressions confront us with the need to protect spheres and public sectors."

The good news is that these sector transgressions have brought more civil-society organizations into the fray. Whereas advocacy groups that are focused on digital rights, such as Algorithm Watch and Mozilla, have long campaigned against big tech's influence, new actors that are focused on labor or migrant issues may now find themselves taking sides. It is in fact one of the recommendations of the Global Data Justice report<sup>1</sup> that digital-rights groups need to coordinate and join forces with sectoral organizations such as trade and student unions and human-rights groups that are not yet focused on digital rights.

Current national and transnational public policy developments, such as the EU AI Act and the US Algorithmic Accountability Act introduced by the US Congress (which are compared side by side in a Correspondence in this issue by Jacob Mokander and Luciano Floridi) focus mainly on addressing possible harms of automated algorithms that affect individual people. However, human-rights non-governmental organizations such as Amnesty International have argued that viewing the potential harms of algorithms through the lens of international human rights offers a more holistic view than does assessing their impact on individual privacy or attempting to mitigate bias<sup>3</sup>. With tech companies now rapidly establishing digital dependencies for goods and services that are essential to society, often while embracing privacy-preserving approaches, a shift of focus on regulation in artificial intelligence is urgently needed. 

Published online: 22 June 2022 https://doi.org/10.1038/s42256-022-00507-2

## References

- López, L., Martin, A., Ohai, F., De Souza, Siddharth P. & Taylor, L. *Global Data Justice* https://globaldatajustice.org/gdj/2637/ (May 2022).
- 2. Sharon, T. Ethics Inf. Technol. 23, 45-57 (2021).
- McGregor, L., Murray, D. & Ng, V. International Human Rights Law as a Framework for Algorithmic Accountability (Cambridge Univ. Press, 2019).