HHR
Health and Human Rights Journal

VIEWPOINT

Technology, Health, and Human Rights: A Cautionary Tale for the Post-Pandemic World

RAJAT KHOSLA

Technology is widely known for moving fast and breaking things, to paraphrase Mark Zuckerberg. Indeed, technology is fast moving into each and every aspect of our life, especially our health and well-being. The COVID-19 pandemic has shown how technology can and should play an important role in helping stop the spread of the disease, including by disseminating public health messages and increasing access to health care (for instance, through virtual consultations). However, the pandemic has also demonstrated how certain governments—in the name of combatting the disease—have rushed to expand their use of surveillance technologies to track individuals and even entire populations. Without human rights safeguards and meaningful public consultation, digital health technologies threaten privacy, freedom of expression, and freedom of association, thus violating rights and degrading trust, which also undermines the effectiveness of such technologies. At Amnesty Tech (a program of Amnesty International), we are taking stock of all that is broken in the technology and health and human rights nexus, while trying to ensure that critical human rights safeguards are put in place.[1]

As we contend with the growing adoption of technology as a tool to address COVID-19, we should learn from past experiences and ensure that health and human rights are protected every step of the way. Within this context, we have identified three growing human rights concerns.

The first is the increasing use of technology to expand surveillance by states, including through access to data collected for public health. Earlier this year, many groups, including Amnesty Tech, raised the alarm about privacy with regard to the rollout of contact tracing apps. Our investigation confirmed that the alarm was well founded, as it discovered major privacy problems in contact tracing apps being used or developed by Qatar, Norway, Bahrain, and Kuwait.[2]

Among the most concerning was the use of centralized systems, wherein governments retain the data gathered by the apps on a central server, making it harder to protect the data from being shared or misused in ways that could lead to human rights abuses.

Over the past few years, Amnesty Tech has uncovered extensive examples of state authorities and others unlawfully using digital surveillance to spy on, intimidate, threaten, or silence activists or to locate, detain, or imprison them.[3] State authorities have increased the surveillance and disempowerment of already disadvantaged communities. Among the lessons we take from this is that function creep—the

Rajat Khosla is Senior Director of Research, Advocacy, and Policy at Amnesty International, International Secretariat.

Please address correspondence to the author. Email: rajat.khosla@amnesty.org.

Competing interests: None declared.

tendency of data collected for one purpose to be repurposed for another, unforeseen purpose—is a fundamental component of the human rights risk posed by state surveillance and, as such, needs to be addressed with adequate safeguards. This means, as our research has shown, that we need strong data protection rules, legal safeguards, and meaningful regulation of the surveillance industry as we enter this new world of massive collection of data within the context of public health concerns.[4]

Unfortunately, we are already seeing rumblings of such government abuse. For example, Israeli authorities attempted to grant the security services access to contact tracing data.[5] While this proposal appears to have been withdrawn, a look at the United States gives a dire warning of where such data sharing could lead. In the United States, the Immigration and Customs Enforcement Agency uses technologies provided by Palantir, a secretive tech giant, to conduct immigration raids that have led to hundreds of arrests, deportations, and family separations.[6] In April 2020, Palantir won a contract with the Department of Health and Human Services to build the "Protect Now" platform aggregating over 187 different data sources from the government and private sector. Given previous examples of the Department of Health and Human Services sharing data with Immigration and Customs Enforcement Agency, policies and practices around the use of technology within the context of public health pose serious concerns, especially for groups that are in particularly vulnerable situations.[7]

In response, Amnesty Tech continues to make targeted and mass state surveillance an ongoing focus of our work, both in our investigations via our Digital Security Lab (which leads technical investigations into cyber attacks against civil society and provides critical support when individuals face such attacks) and in our advocacy and legal efforts, while taking account of the new ways in which states' use of technology to respond to the pandemic may exacerbate these harms globally.

The second cause for concern is the ways in which employers can potentially abuse employee health data. Can an employer be allowed to demand that employees take COVID tests or to reveal their status? How can an employer use this information, and with whom can it be shared? Furthermore, existing regulations governing the collection and use of health data have not kept pace with a rapidly changing economy, especially in the United States. For instance, a gig worker may have very different legal protections or face other vulnerabilities than a contract employee. The intersection of the right to health and privacy requires more robust data protection standards.

Amnesty Tech is analyzing existing legislation and upcoming efforts that may offer protection in some circumstances across jurisdictions governed by differing data protection frameworks, in order to inform our work to ensure human rights-compliant safeguards in these new contexts.

The third cause for concern is health data taking on a key role in the expansion of the surveillance-based business model that dominates the tech sector, whereby people's digital data are bought and sold as a commodity. It is crucial to understand that these risks and harms take place against the backdrop not only of this business model but of a generally thinly regulated marketplace in data. As we pointed out in our report *Surveillance Giants*, the internet is dominated by companies whose primary means of earning profit is through advertising sales premised on their ability to collect, analyze, and draw inferences from massive amounts of our personal data.[8]

Consider the issue of gathering and using health data to sell for advertising purposes. While this practice did not start with the pandemic, it has accelerated during this time. Numerous firms have been collecting health data from consumer products for some time now, including from a wearable fitness trackers, genetic test kits, and myriad other products. This valuable data can fuel analytics aimed at predicting consumer habits or choices and can be purchased to increase data companies' resources and value. In 2019, Fitbit's CEO stated that "ultimately Fitbit is going to be about the data" rather than its hardware or devices.[9] In 2020, Google acquired the company for US$2.1 billion.[10]

This massive accumulation of personal data

usually occurs without individual consent (or with "consent" that is far from adequate under most data protection regimes), but the risk of harm is compounded when the data in question can be resold or shared without adequate safeguards. Moreover, the data are often useful insofar as they provide the basis for predictions about our behavior. While the underlying data themselves may be subject to protections in some jurisdictions, the inferences based upon them often are not, creating a particularly complex scenario.[11]

Inferences that are created based on personal health data—"emergent medical data"—carry tremendous risks for human rights.[12] A health insurer may deny coverage based on a prediction made about a person to which they never consented and may not even know about. Likewise, artificial intelligence can monitor people's movements to track the spread of infectious disease or purchases to track a person's pregnancy status. Just as worrying is how frequently these predictions are inaccurate.[13] Moreover, without proper data subject rights or other avenues via which to claim a remedy, we are left without much recourse.

In response, Amnesty Tech continues to push for a human rights-respecting business model for the internet, as well as safeguards for AI and machine learning systems, such as the Toronto Declaration, which highlights principles for protecting the rights to equality and nondiscrimination in machine learning systems.[14] We will do this while continuing to expose and oppose the harms created by the current business model, as well as any additional harms that may emerge from extensive and invasive analysis of our health data and the uses of the inferences that flow from them.

Our rights to health and privacy are now more interlinked than ever before. Health data pose significant risks at the intersections of state surveillance, a surveillance-based internet, and data protection. All of these lack adequate safeguards to protect the rights at risk. George Orwell once said, "Who controls the past controls the future. Who controls the present controls the past." Without adequate safeguards and protection of rights in the digital space, we risk the health and well-being not only of people today but also of future generations.

Acknowledgments

I would like to thank Joshua Franco, Tamaryn Nelson, and Rasha Abdul Karim for their inputs on the draft manuscript.

References

1. Amnesty International, *Amnesty Tech*. Available at https://www.amnesty.org/en/tech.

2. Amnesty International, *Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.* (June 16, 2020). Available at https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/.

3. Amnesty International. *When best practice isn't good enough: Large campaigns of phishing attacks in Middle East and North Africa target privacy conscious users* (December 19, 2018). Available at https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough.

4. Amnesty International, *We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands* (September 29, 2020). Available at https://www.amnesty.org/en/documents/eur35/2971/2020/en/; Amnesty International, *Ending the targeted digital surveillance of those who defend our rights: A summary of the impact of the digital surveillance industry on human rights defenders* (London: Amnesty International, 2019).

5. J. Breiner and J. Lis, "Israel seeks to give police unrestricted access to Covid contact tracing data," *Haaretz* (October 25, 2020). Available at https://www.haaretz.com/israel-news/.premium-israel-seeks-to-give-police-unrestricted-access-to-covid-contact-tracing-data-1.9261494.

6. Amnesty International, *Failing to do right: Urgent need for Palantir to respect human rights* (London: Amnesty International, 2020).

7. M. Kleinman and C. Krishnaswami, "Why are we trusting a company with ties to ICE and intelligence agencies to collect our health information?," *Washington Post* (May 21, 2020). Available at https://www.washingtonpost.com/opinions/2020/05/21/why-are-we-trusting-company-with-ties-ice-intelligence-agencies-collect-our-health-information/.

8. Amnesty International, *Surveillance giants: How the business model of Google and Facebook threatens human rights* (London: Amnesty International, 2019).

9. L. Dignan, "Fitbit's healthcare unit to deliver $100 million in revenue in 2019," *ZDNet* (February 27, 2019). Available

at https://www.zdnet.com/article/fitbits-healthcare-unit-to-deliver-100-million-in-revenue-in-2019.

10. Fitbit, *Fitbit to be acquired by Google* (press release, November 1, 2019). Available at https://investor.fitbit.com/press/press-releases/press-release-details/2019/Fitbit-to-Be-Acquired-by-Google/default.aspx.

11. T. O'Carroll, "The pandemic could obliterate a last frontier in our privacy," *Newsweek* (July 14, 2020). Available at https://www.newsweek.com/biological-privacy-big-tech-tracing-coronavirus-1517576.

12. Emergent Medical Data, *Health information inferred by artificial intelligence*. Available at https://emergentmedicaldata.com/.

13. E. Pitini, C. De Vito, C. Marzuillo, et al. "How is genetic testing evaluated? A systematic review of the literature," *European Journal of Human Genetics* 26/5 (2018), pp. 605–615.

14. Amnesty International, *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems* (2018). Available at https://www.amnesty.org/en/documents/pol30/8447/2018/en/.