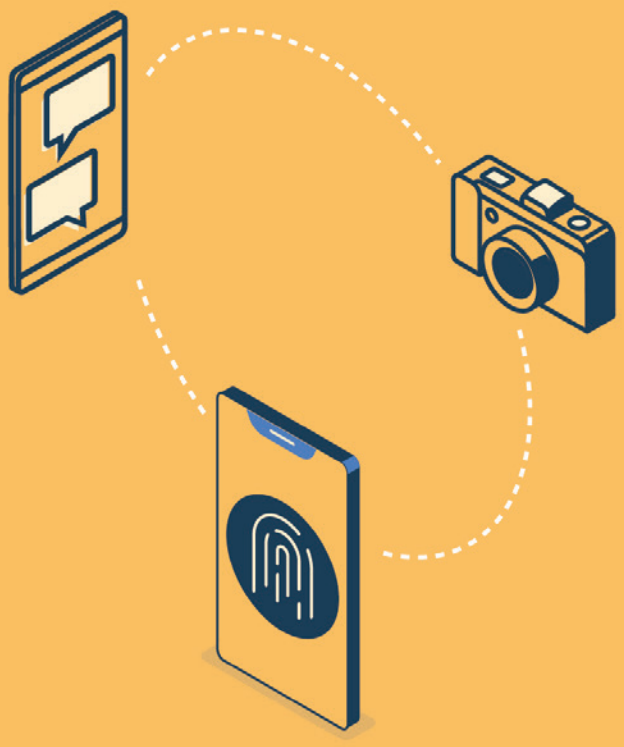
Public Health, Big Tech, and Privacy

Squaring the Contact-Tracing Circle

By Mallory Knodel



Multistakeholder governance—the idea that the state, private sector, and civil society should jointly manage key public goods—has for many years been the lodestar of efforts to secure the internet's democratic future. But is this model a viable mechanism to address the challenges of a global pandemic?

To ensure the best possible response to this worldwide public health crisis, democratic governments should follow an informed, principled approach that strengthens public health infrastructure, minimizes private data collection, and is narrowly designed for the COVID-19 pandemic. The private sector should assist strong government leadership and support a public health vision, and civil society, technology, and health experts should advocate for technology development in the public interest.

In March 2020 alone, civil society, the private sector, and governments launched several noteworthy, joint public-health initiatives to respond to the COVID-19 crisis. The MIT Media Lab created the Private Kit: Safe Paths app with help from Harvard, Facebook, and Uber. Privacy International analyzed an early joint effort between a German tech startup and the Hannover School of Medicine. MTX Group Inc. announced it was working with the New York State Department of Health on New York–specific measures for the company's donated COVID monitoring app.[1] MIT's Bluetooth effort (PACT) is a strong example of an early tech-led joint effort: leadership of the project is shared among MIT institutions, the MGH Center for Global Health, and Harvard Medical School,[2] leading to the design of the now well-known Google/Apple exposure notification platform for contact tracing apps that rely on Bluetooth to indicate proximity of exposure. However, there is no question that digital technology and data collection have been and are being used to expand illiberal and authoritarian regimes of mass surveillance and oppression. When the COVID-19 pandemic presented an unprecedented opportunity for those regimes to expand, groups like the American Civil Liberties Union and the Center for Democracy and Technology sprang into action to develop principles for tech-assisted contact tracing and a task force on coronavirus data, respectively, among other advocacy efforts to ensure responsible technology use and data collection.[3]

As of the end of July 2020, 48 countries confirmed that they had deployed contact tracing or other coronavirus-related tracking apps. This information came from government or developer announcements, verifiable news sources, or published research collected by MIT.[4]

Not all of these tech products, however, have altruistic public health goals at the forefront of their response. Some trackers have an explicitly political aim. For example, an up-to-date database specifically documents the privacy concerns of 154 COVID-related apps available on the Google Play Store.[5] A helpful visualization, accompanied by a formal report, tracks surveillance and civil rights infringements linked to COVID-19 responses.[6]

Reviewing the Implications for Democracy and Human Rights

These technological responses and criticisms demonstrate both the demand for and the concerns associated with public health data collection platforms. Yet as the COVID-19 pandemic continues to affect nations worldwide, one key question appears: what are the rights implications of these responses?

First, there are concerns that the novel coronavirus may never be contained with a vaccine and therefore will pose a persistent threat to public health—in which case society may need to draw lessons from other containment and contact tracing scenarios, such as that used for individuals with HIV/AIDS.[7] Second, even before the pandemic the use of biometric data brought to light the need to contain the unique risks to privacy and individual liberty associated with such personal information being handed over for corporate use.[8] Although advocates ensured that the Google/Apple exposure notification system (in which Bluetooth is used to detect proximity and exposure data is stored locally on a user's device) was narrowly designed for use in the COVID-19 pandemic, those tech giants now have the sole power over whether, if ever, they will decommission the platform and refrain from repurposing it.[9] Other persistent risks not directly related to surveillance include a general sense of public fear, uncertainty, and distrust toward information technology, governments, personal electronic devices, and the media. It seems the crisis has not been wasted by the many ill actors looking to exploit collectively vulnerable societies.

Other persistent risks not directly related to surveillance include a general sense of public fear, uncertainty, and distrust toward information technology, governments, personal electronic devices, and the media.

Although most technology-assisted contact tracing applications originated in the private sector, many have been implemented and executed by governments. Of course, different government agencies bring different mandates, perspectives, and expertise to policy problems, and so the specific agencies involved are also relevant to the discussion: in the case of South Korea's quarantine monitoring app, it was developed by the Ministry of the Interior, not the Ministry of Health and Welfare.[10] In fact, most well-documented joint efforts at tech-enabled responses have been led by central or local governments, not by national health agencies. In March, the British government sought help from tech companies including Google, Palantir, Uber, Deliveroo, Amazon, Faculty AI, Microsoft, and Apple.[11] In the European Union, the European Commission called for help from telecom providers in March, requesting mobile location data (an alternative to Bluetooth proximity) for the purposes of COVID-19 response.[12] The U.S. government also had early conversations with its powerhouse technology sector in an effort to strengthen joint responses.[13]

Despite this outreach, there were early derailments. In the United States, for instance, the decentralized state-by-state approach posed a particular challenge to joint health and tech efforts, which may explain why tech-assisted contact tracing did not become widespread there.[14] In China, the AliPay Health Code app raised privacy concerns for sharing data with local authorities, creating trust issues among users whose authoritarian government gives them no obvious means to challenge the app's use or design.[15] The ways in which different governments approach partnerships and select companies with which to partner also have implications for privacy, democracy, and human rights. Partially as a result of these factors, in some cases technical design choices made by private sector partners have superseded those made by governments. Citizens are left to ask themselves: is it appropriate for unelected private corporations to control this kind of politically sensitive infrastructure?

On the whole, many of these technology-assisted efforts to track, monitor, and contain the pandemic have failed in their professed goals, yet governments nonetheless continue to encourage their use. Unsurprisingly, watchdog organizations continue to sound the alarm about data privacy concerns. Privacy International describes civil society concerns about Colombia's coronavirus information and identification app, developed and launched by the Colombian National Health Institute. Local civil society groups like Fundacion Karisma expressed strong concerns about the app's surveillance potential and accessibility.[16] Before debating any of the governance tradeoffs involved in technological interventions during the pandemic, one first must ask: have there been any successes? And what are the measures of that success? If the strengthening of public health infrastructure is the measure, there have been notable failures, undermined by a tug-of-war between national governments and private sector market power.[17]

In some ways, privacy issues are interconnected with larger questions about the accountability and ownership of these systems. In the case of the Google/Apple exposure notification system, many countries did not use their sovereign and regulatory powers to limit tech companies; they took the companies' word at face value.[18] Independent researchers came to the same conclusion. Researchers at Trinity College in Dublin recommended that the Google/Apple system have more oversight: "A governance setup that imposes a similar level of scrutiny over both the client app component and the Google/Apple component of the [system] seems sensible and necessary" owing to the risk of inadequate privacy protections by companies, which are already subject to criticism over privacy implications.[19]

The key principles for tech-enabled COVID-19 interventions advocated by civil society organizations... may well be fundamentally at odds with a government-administered infrastructure that can fully control a crisis.

Some observers have argued that preventing undue private sector influence on jointly governed initiatives will require "creating a complex institutional architecture" capable of scrutinizing technological applications and improving public technical literacy.[20] Indeed, there are increasing calls for privacy and public health experts, such as the Pan-European Privacy-Preserving Proximity Tracing proposal, to work together to ensure proper rollout and continued oversight of public health technology.[21]

Toward a More Perfect MultiStakeholder Approach

The key principles for tech-enabled COVID-19 interventions advocated by civil society organizations—that they be, among other things, voluntary, nonpunitive, private, nondiscriminatory, and decentralized—may well be fundamentally at odds with a government-administered infrastructure that can fully control a crisis.[22] If this is the case, who should navigate the necessary tradeoffs? The answer cannot be one sector alone. The response must cooperative, collaborative, and jointly managed.

What are the obvious worst things to avoid when designing multistakeholder initiatives for technological challenges? Certainly, joint governance can complicate coordination and interoperability.[23] But the most serious issue to avoid is the potential to create a façade of accountability, one which gives the appearance of appropriate oversight while in effect allowing relatively free reign.[24] Many multistakeholder responses fail to demonstrate appropriate levels of transparency. No matter how useful these responses might be, they are

liable to undermine inclusivity, diminish the space for civil society consultation, exacerbate existing inequalities (such as gender discrimination), and potentially undermine public trust in the public health response.[25]

In sum, and for the longer term, better governed tech-assisted solutions to public health crises can improve the confidence of governments in their ability to respond and help check private sector motivations that are not aligned with the public interest. This essay has largely focused on countries with the best-case political climates, but further research is needed on outcomes and trends in nondemocratic countries and in the Global South. Another area for future research is the ways in which technological governance may have accelerated illiberal trends within democracies through a climate of digital inequality, disinformation, mass surveillance, and cybersecurity threats. These and other perspectives will require continued attention as the COVID-19 pandemic continues to have deleterious effects on individuals, communities, and nations around the world.

Endnotes

1 Will Douglas Heaven, "A New App Would Say If You've Crossed Paths with Someone Who Is Infected," *MIT Technology Review*, 17 March 2020, www.technologyreview.com/2020/03/17/905257/coronavirus-infection-tests-app-pandemic-location-privacy; "Germany: Geotracking Startup Working with the Hannover School of Medicine on a Data Analysis Platform," Privacy International, 11 March 2020, http://privacyinternational.org/examples/3437/germany-geotracking-startup-working-hannover-school-medicine-data-analysis-platform; Brandi Addison, "Frisco Technology Company Donates Its Disease-Monitoring App to all U.S. Public Schools," *Dallas News*, 13 March 2020, www.dallasnews.com/news/public-health/2020/03/11/frisco-technology-company-has-launched-a-disease-monitoring-app-for-coronavirus-cases.

2 For the leadership and mission statement of this project, see: R. L. Rivest et al., "PACT: Private Automated Contact Tracing Mission and Approach," Massachusetts Institute of Technology (MIT), 19 May 2020, https://pact.mit.edu/wp-content/uploads/2020/05/PACT-Mission-and-Approach-2020-05-19-.pdf.

3 Daniel Kahn Gillmor, *Principles for Technology-Assisted Contact-Tracing*, American Civil Liberties Union, 16 April 2020, www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing; Greg Nojeim, "CDT Statement and Announcement of Coronavirus: Data for Life and Liberty Task Force Formation," Center for Democracy & Technology, 30 April 2020, https://cdt.org/insights/cdt-statement-and-announcement-of-coronavirus-data-for-life-and-liberty-task-force-formation.

4 Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson, "A flood of coronavirus apps are tracking us. Now it's time to keep track of them," *MIT Technology Review*, 7 May 2020, www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker.

5 "COVID-19 App Tracker," retrieved 29 September 2020, https://covid19apptracker.org.

6 "Limitations on Digital Rights and Civic Freedoms in a Pandemic," Pandemic Big Brother, retrieved 30 September 2020, https://pandemicbigbrother.online/static/core/files/Report_Pandemic_Big_Brother.pdf.

7 Rose Saxe, "Contact Tracing and COVID-19: Lessons From HIV," American Civil Liberties Union, 15 May 2020, www.aclu.org/news/hiv/contact-tracing-and-covid-19-lessons-from-hiv.

8 Tanya O'Carroll, "The Pandemic Could Obliterate a Last Frontier in Our Privacy: Our Biological Selves," *Newsweek*, 14 July 2020, www.newsweek.com/biological-privacy-big-tech-tracing-coronavirus-1517576.

9 Andy Greenberg, "How Apple and Google Are Enabling Covid-19 Contact-Tracing," *Wired*, 10 April 2020, www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19.

10 Max S. Kim, "South Korea Is Watching Quarantined Citizens with a Smartphone App," *MIT Technology Review*, 6 March 2020, www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine.

11 Jim Waterson, "Boris Johnson Urges Top UK Tech Firms to Join Coronavirus Fight," *The Guardian*, 13 March 2020, www.theguardian.com/business/2020/mar/13/johnson-urges-top-uk-tech-firms-to-join-coronavirus-fight.

12 Mark Scott, Laurens Cerulus, and Laura Kayali, "Commission Tells Carriers to Hand Over Mobile Data in Coronavirus Fight," *Politico*, 25 March 2020, www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19.

13 Tony Romm, Elizabeth Dwoskin, and Craig Timberg, "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus," *Washington Post*, 18 March 2020, www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus.

14 Gregory Barber and Will Knight, "Why Contact-Tracing Apps Haven't Slowed Covid-19 in the US," *Wired*, 8 September 2020, www.wired.com/story/why-contact-tracing-apps-not-slowed-covid-us.

15 Paul Mozur, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," *New York Times*, 7 August 2020, www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.htm.

16 "Colombia: Coronapp Fails at Public Information Purpose," Privacy International, 9 March 2020, http://privacyinternational.org/examples/3435/colombia-coronapp-fails-public-information-purpose.

17 Michael Veale, "Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit," *The Guardian*, 1 July 2020, www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights.

18 Casey Newton, "Why Countries Keep Bowing to Apple and Google's Contact Tracing App Requirements," *The Verge*, 8 May 2020, www.theverge.com/interface/2020/5/8/21250744/apple-google-contact-tracing-england-germany-exposure-notification-india-privacy; Veale, "Privacy Is Not the Problem."

19 Douglas J. Leith and Stephen Farrell, "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps," Trinity College Dublin, 18 July 2020, www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf.

20 Maria Savona, "The Saga of the Covid-19 Contact Tracing Apps: Lessons for Data Governance," SWPS 2020-10, 7 July 2020, https://doi.org/10.2139/ssrn.3645073.

21 Carrie DeCell, "Can Governments Track the Pandemic and Still Protect Privacy?," Just Security, 6 April 2020, www.justsecurity.org/69549/can-governments-track-the-pandemic-and-still-protect-privacy.

22 "ACLU Issues Governance Principles for COVID-19 Contact Tracing Technologies," American Civil Liberties Union, 18 May 2020, www.aclu.org/press-releases/aclu-issues-governance-principles-covid-19-contact-tracing-technologies.

23 Jens-Henrik Jeppesen and Pasquale Esposito, "COVID-19: European Data Collection and Contact Tracing Measures," Center for Democracy & Technology, 29 April 2020, https://cdt.org/insights/covid-19-european-data-collection-and-contact-tracing-measures.

24 "COVID-19 Rapid Evidence Review: Exit through the App Store?," Ada Lovelace Institute, 20 April 2020, www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf.

25 Dheepa Rajan et al., "Governance of the Covid-19 Response: A Call for More Inclusive and Transparent Decision-making," *BMJ Global Health* 5, no. 5 (5 May 2020), e002655, https://doi.org/10.1136/bmjgh-2020-002655.