COVID-19 APPS ARE TERRIBLE—THEY DIDN'T HAVE TO BE

Jane Bambauer & Brian Ray[*]

November 2020

COVID-19 apps in the United States have been ineffective as public health tools because they are designed primarily to protect privacy. Poor design choices, effectively mandated by Google and Apple, were driven by ongoing consumer privacy and national security debates that shortsightedly rejected tracking technologies.

During March and April 2020, we watched with growing unease as China, South Korea, and Israel dramatically expanded government surveillance to contain the spread of the novel coronavirus.[1] In these early weeks of the pandemic—as the U.S. surpassed Italy to lead the world in coronavirus deaths, millions of small businesses faced permanent closure from lockdown restrictions,[2] and the unemployment rate skyrocketed from 3.8 percent to 14.4 percent—American observers routinely worried that U.S. government agencies might expand surveillance under the cover of public health in similar ways that national security was used after 9/11. "As coronavirus surveillance escalates, personal privacy plummets," warned the *New York Times*.[3]

[*] Professor of Law, University of Arizona; Leon M. and Gloria Plevin Professor of Law, Cleveland-Marshall College of Law.

[1] See Catalin Cimpanu, "US, Israel, South Korea, and China Look at Intrusive Surveillance Solutions for Tracking COVID-19," ZDNet, March 20, 2020, www.zdnet.com/article/us-israel-south-korea-and-china-look-at-intrusive-surveillance-solutions-for-tracking-covid-19/.

[2] Greg Iacurci, "7.5 Million Small Businesses Are at Risk of Closing, Report Finds," CNBC, April 14, 2020, www.cnbc.com/2020/04/14/7point5-million-small-businesses-are-at-risk-of-closing-report-finds.html.

[3] Natasha Singer and Choe Sang Hun, "As Coronavirus Surveillance Escalates, Personal Privacy Plummets," *New York Times*, March 23, 2020, www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

In fact, as we see it, state and federal governments (as well as influential private firms) did exactly the opposite, prioritizing a fetishized notion of individual privacy over collective public health. They actively distanced themselves from the use of digital contact-tracing and infection-risk-scoring tools. The reluctance to leverage communications technologies to stem the spread of the novel coronavirus was so strong and so pervasive that the COVID-19 apps in operation today are underpowered and undersubscribed by design. They languish on a few phones and in app stores as the ghosts of clever programming.

The two of us were among the thousands of well-intentioned people who came together across multiple companies, government agencies, and nonprofits to identify creative ways to responsibly use technology to limit the death and social destruction of COVID-19. We watched with growing dismay as intersecting forces caused each institutional player to rationally and understandably prioritize individual privacy interests at the expense of developing new technological tools that could curb the pandemic and enable the United States to reopen safely.

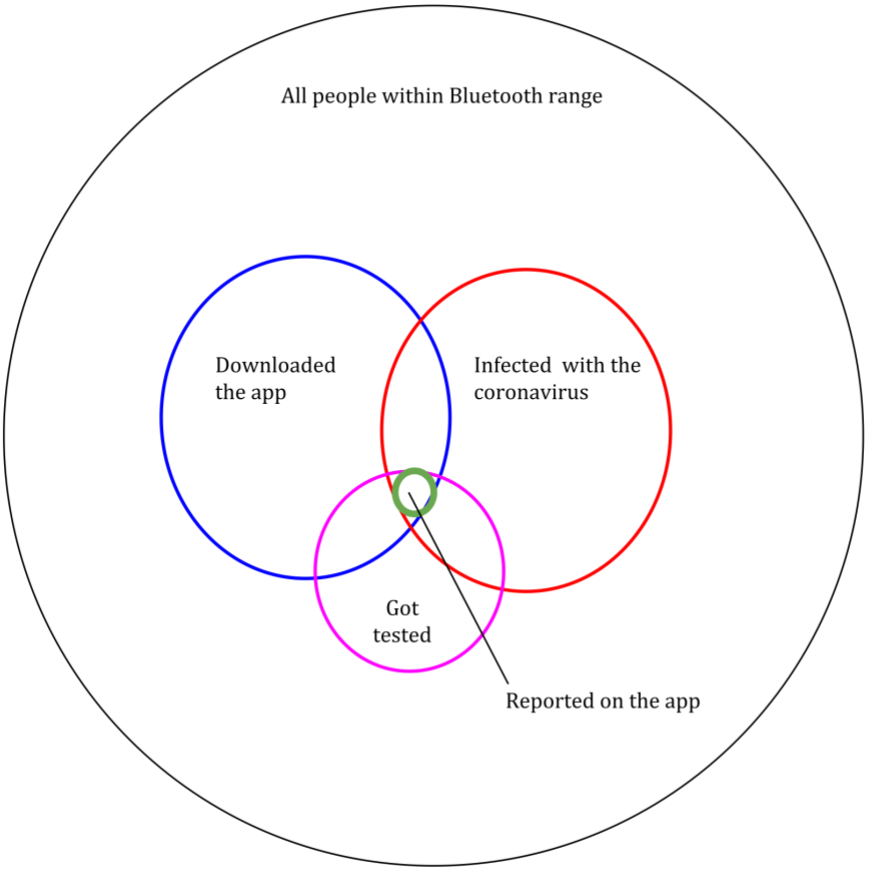
Take, for example, the development of the Covid Watch Arizona app, currently in use at the University of Arizona, and one of only a handful of apps that Apple and Google permit to use their Bluetooth-based exposure notification system.[4] Although the university advises students and staff to download the app, the enthusiasm even among top administrators is tepid, and for good reason. The app is destined to be useless. The top design mission wasn't the effective tracking and tracing of the virus but, rather, achievement of a near-zero privacy risk. The app collects *only* Bluetooth-enabled proximity data—a string of numbers representing the randomly generated IDs of nearby phones. It *does not* collect identifying information, GPS information, or any other data. Even the positive coronavirus test results that are necessary to trigger an exposure notification are difficult for the app to collect: Users have to choose to report their results and wait for public health authorities to verify them.[5]

The result of this privacy-above-all design is a tool that only rarely provides users with any information at all. The app will notify users about a possible exposure event only if the infected person is among the small percentage of people who also downloaded the app, received a clinical diagnosis, and then bothered to use the app to report that result.

---

[4] Apple-Google, "Exposure Notification: Frequently Asked Questions v1.2, September 2020, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf.

[5] See Apple-Google, "Exposure Notification."



Even in that lucky scenario, users will receive information only if they happen to open the app and check for in-app notifications. And, even if users happen to *do that,* the app will provide limited information about the exposure event—the day it occurred and the risk the algorithm assigns. That risk is based solely on the strength and duration of the Bluetooth signal, which provides a noisy approximation of the length of the exposure and the distance between the two individuals. It doesn't incorporate any other useful information, even basic location information that could allow the user to figure out whether she was indoors or outside or wearing a mask, or even left the phone in another room.

Users who affirmatively *want* to allow the app to include even the basic GPS-location information that their phones likely already routinely collect—so that they or others they come into contact with could know the context of the exposure—are out of luck. A combined GPS and Bluetooth

system could enable much better risk scores and substantially reduce the number of false-positive notifications, but the Covid Watch app's privacy-at-all-costs design uses proximity data alone.[6]

In spite of its substantial limitations, the app could still add some small value to the university's pandemic response, but that value is speculative and constrained.[7] And so, when the entirely predictable outbreaks of COVID-19 occurred in Tucson following the also-predictable socializing of college students, the university imposed shelter-in-place orders and threatened punishment-based enforcement of mask and social distancing rules. But it did not compel (or even strongly urge) the use of the Covid Watch app. The unstated understanding is that the app is performative, like the plexiglass barriers that separated the vice-presidential candidates during their debate: a highly visible but largely ineffective ornament for the COVID-19 response.[8]

The university made no serious effort to use apps and big data to keep its community safe, but it cannot be blamed for this omission. By the time the University of Arizona (and other universities in the state) were coordinating with Covid Watch to design an app, most of the opportunities to harness digital tech already were closed. Google and Apple imposed a de facto universal technical standard on the world by tightly restricting how apps permitted to use the companies' co-developed Bluetooth capability would function. Since those two companies are responsible for the operating systems of nearly every smartphone in the world, the companies wielded great power over the functionality of COVID-19-related apps, and they used that power to demonstrate their fealty to certain specific forms of data privacy. Google and Apple decided that any app that makes use of their low-powered Bluetooth proximity detection had to keep the data decentralized (on each user's phone) and could not merge GPS or any other form of data with the proximity data.[9]

---

[6] See Ramesh Raskar et al., "Adding Location and Global Context to the Google/Apple Exposure Notification Bluetooth API," Arxiv, July 25, 2020, https://arxiv.org/pdf/2007.02317.pdf.
[7] See Stewart Baker, "The Problem With Google and Apple's COVID-19 Tracking Plan," *Lawfare,* April 14, 2020, www.lawfareblog.com/problem-google-and-apples-covid-19-tracking-plan.
[8] See, e.g., Natasha Singer, "Virus-Tracing Apps Are Rife With Problems. Governments Are Rushing to Fix Them," *New York Times*, July 8, 2020, www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html. This is similar to what Bruce Schneier has dubbed "security theater," the use of visible but largely useless security measures to make people feel safe. See Bruce Schneier, "Beyond Security Theater," November 2009, https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html.
[9] Darrell Etherington, "Apple and Google Release Sample Code, UI and Detailed Policies for COVID-19 Exposure-Notification Apps," Tech Crunch, May 4, 2020, techcrunch.com/2020/05/04/apple-and-google-release-sample-code-and-detailed-policies-for-covid-19-exposure-notification-apps/.

Admittedly, Google and Apple are not entirely to blame. Both companies have to comply with European laws and guidance that strongly discourage any potentially unnecessary data collection or sharing. Perhaps more relevant than the laws in Europe or elsewhere, though, is the cultural and political climate that swirls around the two companies. After all, while nearly every privacy law contains an exemption for public health emergencies (European law included), there is no exemption to the public contempt and distrust that the companies themselves have built over time.[10]

Google and Apple could have been relieved of this awkward position if lawmakers affirmatively *required* them to enable or create high-efficacy COVID-19-risk apps during the pandemic, but this was so politically controversial that some members of Congress instead called for *prohibiting* even their protective-to-a-fault tool, putting beyond discussion the sort of apps that could have a fighting chance of helping to reduce health risks even while states were relaxing their lockdown measures.[11] The European Data Protection Board, as well as several U.S. state and local governments already greatly constrain the sort of data collection and automation that could most effectively support contact tracing.[12] Politically, coming out in favor of a new surveillance program, no matter its design, seemed to be impossible under the prevailing climate of distrust.

That left schools, retailers, and employers as the only plausible candidates to aggregate a demand for effective COVID-19 apps, but they, too, faced a mix of incentives. Every campus, retailer, and employer wants to do what they can to keep their community safe. But, given public backlash against sensible policies like mask requirements, it would be recklessly out of line with public sentiment for any private entity to use its market power to encourage the creation or adoption of a more data-intensive app.

And since Apple and Google erected barriers to the creation of effective COVID-19 apps, and since the U.S. government is reluctant to even endorse the use of health surveillance tools (let alone

---

[10] See, e.g., Mike Feibus, "Are Coronavirus Contact Tracing Apps Doomed to Fail in America?" *USA Today,* June 24, 2020, www.usatoday.com/story/tech/columnist/2020/06/24/apple-google-contact-tracing-apps-privacy/3253088001/.

[11] See, e.g., Kerry Pickett, "'Totalitarianism': Congressman Calls Method to Track Coronavirus Cases an Invasion of Privacy," In the News, April 16, 2020, https://biggs.house.gov/media/in-the-news/totalitarianism-congressman-calls-method-track-coronavirus-cases-invasion-privacy.

[12] European Data Protection Board, *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak,* April 21, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; and Dave Perera, "South Carolina Legislature Puts Coronavirus Apps on Hold," MLex, June 26, 2020, mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/south-carolina-legislature-puts-coronavirus-apps-on-hold.

financially support or require them), there is no chance any private actor will face serious risk of liability for *failing* to develop or adopt an effective COVID-19 app.

Thus, a mix of complex and deeply rooted social preconditions caused the United States to squander an opportunity to make wide-scale use of data for pandemic management. Our analysis provides a postmortem.

First, we make the case that apps requiring modest privacy trade-offs have a proper place in disease surveillance. As we explain, communications technology could have been a valuable asset, working alongside masking requirements, adequate testing, and traditional contact tracing, to obviate a bitter choice between health risks and social isolation. This does not mean the United States would have had to go to the same lengths that China or even South Korea did to extract all (maybe even more) of the value of single-purpose data surveillance. To the contrary, a killer app would have been more likely to emerge if there was a privacy framework in place for public health technology. Since the management of a pandemic does not require the sort of secretive government surveillance and data retention that national security does, an efficacious app could have been affirmatively *supported* by strong privacy and accountability guarantees rather than being in conflict with them.

Next, the autopsy. We explain why the United States could not make the policy and technical innovations necessary to let these apps emerge. We investigate four intersecting sources of dysfunction: (a) political hesitance due to preexisting techlash and surveillance politics; (b) public relations problems for Google and Apple; (c) de facto immunity for other actors (including major retailers) that might have invested in a reliable app; and (d) lost interest by the general public.

From these analyses, we derive three lessons to improve preparedness for the next crisis of communicable disease. First, public discourse about privacy (if not in general, at least in the context of public health) should emphasize the trade-offs between individual and collective goals so that the United States does not face the next pandemic with expectations of inflexible individual privacy rights. Second, policymakers should establish certain principles of accountability and transparency for the special context of public health crises. Finally, Congress should enact a set of dormant disease surveillance laws that are activated when the Centers for Disease Control and Prevention (CDC) officially recognize an epidemic from contagious disease so that the data infrastructure and accompanying trustworthy privacy rules are in place at the outset of the crisis.

WHAT SHOULD HAVE BEEN

To understand why contemporary privacy discourse and instincts didn't serve the United States well during the coronavirus pandemic, we start with a thought experiment. Let's start from a clean slate. What would we need from a COVID-19 app if we were going to tackle the most pressing public

health problems? And what would we need to address the most critical privacy risks? Finally, how could these two needs be reconciled?

Meeting Public Health Needs

Technology would assist public health most by providing or improving the following:

- *Reliable measures of risk* that individuals have contracted the coronavirus.
- *Smart recommendations* communicated to individuals based on their particular estimated risk (for example, reducing social activities, getting a COVID-19 test, or immediately self-quarantining).
- *Near instantaneous tracing* of all people who may have come into close contact with infected or high-risk individuals.
- *Swift updating* of those contacts' estimated risk and recommendations.[13]

Instead of focusing on how to achieve these core functions, public debate about COVID-19 apps never got out of the trough of disillusionment. Brookings published a report in April titled "Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis," which concluded that any claims that COVID-19 apps could make a meaningful contribution to the pandemic response were "implausible at best, and dangerous at worst."[14] Yet, of the items on the list of public health needs that apps could have addressed, none is far-fetched. Lest there be any doubt, the public health response in South Korea suggests that tech-assisted improvements were at least *plausible.*

South Korea has avoided lockdowns by making data-driven decisions about who to test, trace, isolate, and quarantine. The government uses multiple independent sources of information—geolocation, credit card data, closed-circuit television, facial recognition, and old-fashioned interviews—to better trace contacts and predict the risk of transmission for each person.[15] This rich and varied data on every individual allows public health officials to quickly update risk assessments;

---

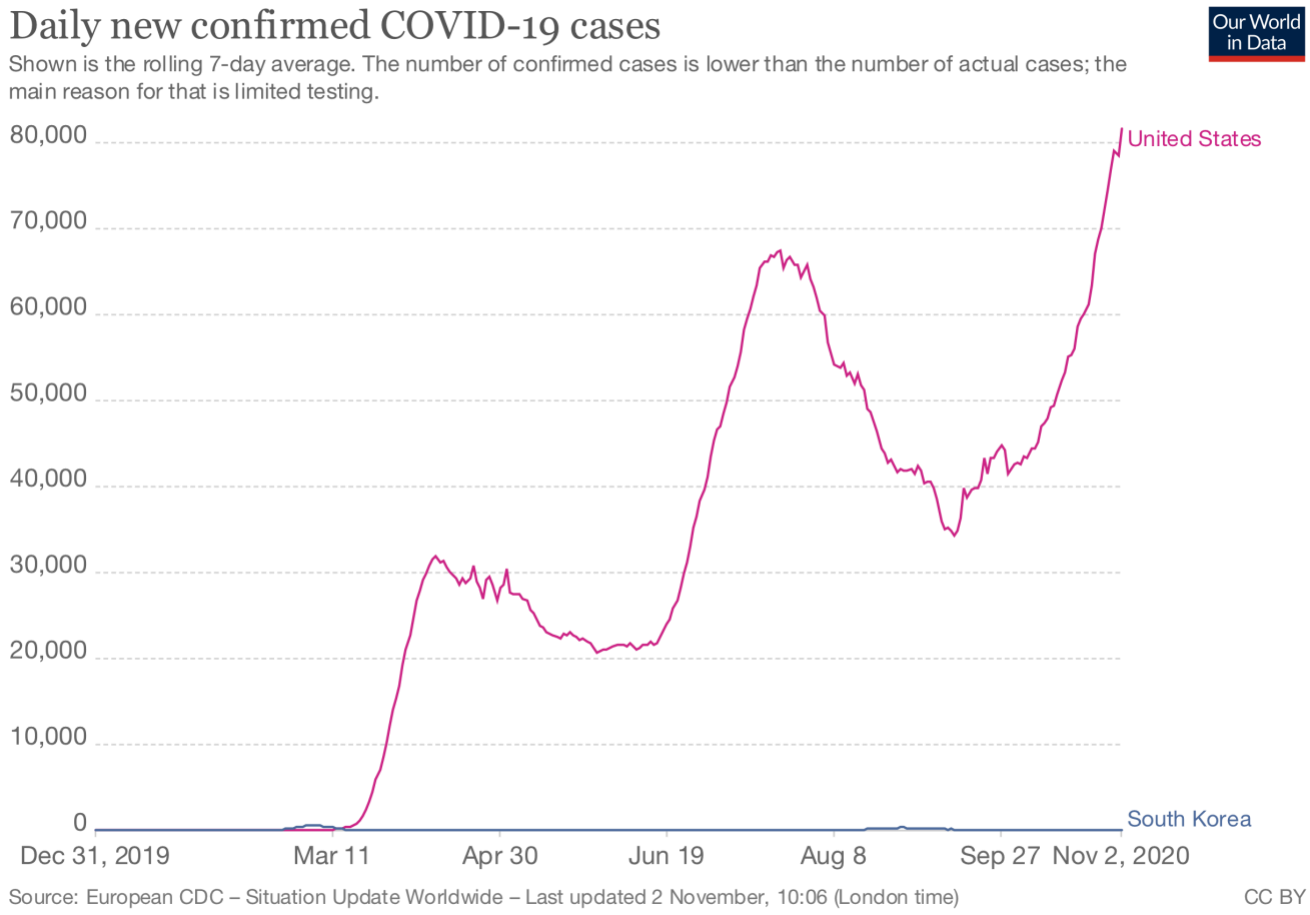
[13] For an extensive analysis of the public health needs that digital contact tracing could assist in meeting, see Jeffrey Kahn, *Digital Contact Tracing for Pandemic Response:* Summary (Baltimore, MD: Johns Hopkins University Press, 2020), 13–14, https://muse.jhu.edu/chapter/2628662/pdf.

[14] Ashkan Soltani et al., "Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis," Brookings TechStream, April 27, 2020, www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[15] Min Joo Kim & Simon Denver, "A 'Travel Log' of the Times in South Korea: Mapping the Movements of Coronavirus Carriers," *Washington Post*, March 13, 2020, www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/ 03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html.

notify high-risk individuals; get them to self-quarantine before infecting others; get them tested as quickly as possible; and, if they test positive, isolate them, decontaminate surfaces likely to be infected, and repeat the process based on *their* contacts.

By any public health measure, South Korea has done a far better job of protecting the health of its residents than the United States has. This was just as true during the so-called "spike" in Korean cases in the fall of 2020.[16]



At one time, the differences between the U.S. and Korean response could have been chalked up to differences in testing capacity, but as testing has ramped up in the United States, it is increasingly obvious that one of the greatest impediments to duplicating South Korea's success is the policy

[16] Max Roser, Hannah Ritchie, Esteban Ortiz-Ospina, & Joe Hasell, "Coronavirus Pandemic (COVID-19)," 2020, OurWorldInData.org.

around disease surveillance. South Korea uses data to narrowly target short-term quarantines so that asymptomatic spread is tamped down without causing quarantine fatigue.[17]

The United States, by contrast, was forced to resort to the unprecedented step of large-scale lockdowns and intermittent mass quarantines that have had widespread, devastating effects on the economy.[18] South Korea and the United States identified their first coronavirus case on the same day. Yet, while the U.S. cumulative case count has reached more than 30,000 per million people and gross domestic product (GDP) is projected to suffer a full-year contraction of almost 4 percent, South Korea has had a mere 500 cases per million and is projected to lose only 1 percent or less of GDP in 2020.[19] Moreover, the crude costs measured in lives, cases, and GDP do not capture the toll in the form of depression, substance abuse, domestic violence, and other social and psychological disorders that broad lockdowns cause.[20]

Mitigating Privacy Risks

Effective disease surveillance tools pose three critical privacy risks that should be minimized and managed:

- *Indefinite storage* of COVID-19-related personal data.
- *Repurposing* COVID-19-related personal data for uses unrelated to managing the public health crisis (especially for high-stakes purposes like general law enforcement, benefits qualifications, or employment).
- *Unauthorized access* to COVID-19-related personal data by any person or entity that does not have a legitimate need related to the public health crisis. (This covers both inadvertent access caused by inadequate data security as well as intentional disclosure by the data controller.)

---

[17] Sangchul Park et al., "Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies," *Journal of the American Medical Association,* 323 (2020): 2129.
[18] Greg Ip, "New Thinking on Covid Lockdowns: They're Overly Blunt and Costly," *Wall Street Journal*, August 24, 2020, www.wsj.com/articles/covid-lockdowns-economy-pandemic-recession-business-shutdown-sweden-coronavirus-11598281419.
[19] Morten Soendergaard Larsen, "COVID-19 Has Crushed Everybody's Economy—Except for South Korea's," Foreign Policy, September 16, 2020, foreignpolicy.com/2020/09/16/coronavirus-covid-economic-impact-recession-south-korea-success/.
[20] Mark É Czeisler et al., "Mental Health, Substance Use, and Suicidal Ideation During the COVID-19 Pandemic — United States, June 24–30, 2020," *Morbidity and Mortality Weekly Report* 69 (2020): 1049–57, www.cdc.gov/mmwr/volumes/69/wr/mm6932a1.htm.

In these respects, South Korea is *not* the model the United States should follow as it renovates its disease surveillance rules. Indeed, the South Korean system has been justly criticized as overly intrusive and heavy-handed. The government collected detailed location history logs of all residents and, for the first several months, routinely published the location histories of all COVID-19 cases publicly. Although the location histories did not have direct identifiers attached, the richness of the data allowed for the reidentification of at least some of the individual COVID-19 patients. Public disclosure of sensitive and sometimes embarrassing information in online forums prompted the country's human rights commission to call for new guidelines to restrict public disclosure.[21] Moreover, quarantines were enforced through police visits, including to anybody who turned off their phone. None of these practices is necessary for an effective data-driven response. Yet these privacy-invasive features tended to steal the focus of public debate, clouding public consideration of the valuable lessons the United States could draw from South Korea's data-intensive program.

Public commentary about COVID-19 apps has uncritically assumed that the privacy risks of automated disease surveillance are high.[22] From the start, the public conversation around apps assumed that the *types* of data they collect should be limited, and that participation in any digital COVID-19 program should be a matter of unpressured, completely voluntary choice. But in the context of a pandemic, individual control over personal data should not obstruct the collective actions that are necessary to respond to an evolving crisis. Instead, it's important to interrogate the legitimate *reasons* why a person would be reluctant to allow the state or private companies to collect, disclose, and use information. Health surveillance is less threatening to life and liberty than is the pandemic itself, especially if individuals have good reason to trust that their data will be accessed by a limited set of actors, for a narrow set of public health purposes, and that it will be destroyed when the health crisis is resolved. If transparent, auditable mechanisms are put in place that strictly limit the use of the modest additional personal data (listed above) solely for health purposes and restrict who can access that information, then unfettered consent is not a necessary element to a responsible data governance plan. And, in any case, without those protections, consent is insufficient to protect rights.

[21] Eun A Jo, "South Korea's Experiment in Pandemic Surveillance," *The Diplomat*, April 13, 2020, thediplomat.com/2020/04/south-koreas-experiment-in-pandemic-surveillance/.
[22] See, e.g., Soltani et al., "Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis."

Trustworthy Pandemic Response

Looking at the public health and privacy "must haves" lists, it's obvious that western countries could have had many of the benefits (and possibly more) that come from aggressive collection and repurposing of data without including the data practices that unreasonably threaten personal privacy. The United States would have been well served by a system that is smart enough to allow algorithms and human contact tracers to work together to formulate tailored warnings and deliver them only to those Americans who may have been infected. This sort of technology-assisted *narrowcasting* can preserve the patient's privacy by communicating only what is necessary (typically, when and where their own potential exposure event took place, or why the individual may be at heightened risk because of several recent low-probability exposure events). This system would achieve most of the public health benefits made possible by automated contact tracing *without* many of the privacy costs associated with South Korea's system.[23]

Ideally, a smart, privacy-protective system would do the following:

- **Collect multiple types and sources of data.** Digital contact tracing could be vastly improved by adding geolocation data to the proximity data collected through the Google-Apple exposure notification system.[24] Location data and proximity detection each have some advantages over the other, so each can make significant contributions to reducing error (both false positives and false negatives). Both geolocation and proximity detection will be unable to definitively determine whether people were close enough to each other to have a credible risk of transmission, but, fortunately, each system's uncertainty is different. This is good, as each can help fill the gaps left by the other.
- **Create a data repository that is reliably and provably constrained by a robust set of privacy and transparency rules.** Proximity data, geolocation data, and medical test results are sensitive on their own, and more so in combination. If the government can make credible promises that the data will be handled according to a reasonable set of rules and standards, those promises would provide the legal backdrop that could allow communications

[23] For an accounting of the privacy costs, see Park et al., "Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies."
[24] See Ramesh Raskar, "Adding Location Context to Apple/Google Exposure Notification Bluetooth API: MIT SafePaths Encryption Proposals for GPS + Bluetooth," Medium, April 26, 2020, medium.com/@rameshboston/adding-location-context-to-apple-google-exposure-notification-bluetooth-api-mit-safepaths-6fe54474835a.

technology companies and individual employers, retailers, and schools to make better use of COVID-19 apps.

- **Allow public health experts to analyze data to make reliable, targeted risk scores and customized public health recommendations.** A system that combines proximity data with GPS data would be able to outperform the risk measures that exist today. Moreover, centralization of data allows for more accurate and timely risk assessment because individuals who are exposed to one or more people who themselves came into contact with someone who tested positive for the virus can be notified and given recommendations calibrated to their circumstances.
- **Maximize and incentivize participation in the program.** Automated risk-scoring, contact tracing, and notifications work better as more people join. Even short of legal mandates requiring individuals to download and run a COVID-19 app (which we wouldn't recommend anyway), the government, private firms, and public health experts can incentivize participation.[25] A stimulus bill, for example, could offer a cash payment or a voucher for cell phone service to anybody who downloads and runs an app. Retailers could have required that entrants both wear a mask and run an app while they shop. At the very least, public health authorities could recommend their use instead of staying neutral or silent.

Each of these elements could be accomplished in a variety of ways that involve sensible trade-offs between the competing priorities of safely reopening activities and protecting privacy. Even a system that incorporated a subset of these elements could substantially improve the anemic COVID-19 apps that are available today. Utah's Healthy Together app used both Bluetooth proximity data and geolocation data when users affirmatively opted in to location tracking until July, when the app stopped supporting geolocation *even with* the voluntary consent of users.[26] The MIT project Safe Paths embraced the use of GPS in conjunction with proximity data, even while self-consciously avoiding any whiff of "Big Brother" by storing all data on individuals' devices unless and until they tested positive (rejecting the second and third points, above).[27] The Safe Paths team has also stated that consent to use a COVID-19 app should be exercised free from any pressure (rejecting the fourth

[25] Incentives could result in broad adoption without causing the irk, backlash, and noncompliance that a national mandate might provoke.

[26] Bethany Rodgers, "Utah's Expensive Coronavirus App Won't Track People's Movements Anymore, Its Key Feature," *Salt Lake Tribune*, July 11, 2020, www.sltrib.com/news/politics/2020/07/11/states-m-healthy-together/.

[27] MIT Media Lab, "Safe Paths: A Privacy-First Approach to Contact Tracing," *MIT News*, April 10, 2020, news.mit.edu/2020/safe-paths-privacy-first-approach-contact-tracing-0410.

point, above). If a service is conditioned on a person's use of a COVID-19 app, this, the team claims, is "a lack of real choice."[28] Nevertheless, by acknowledging the practical need to combine proximity data with geospatial data, Safe Paths represents an eminently more sensible position within the debates on COVID-19 technology.

BARRIERS

In this section, we explain the collective failure of American COVID-19 apps through four barriers—four political, legal, and cultural hindrances that reflexively pushed digital COVID-19 tech into paralysis.

Barrier 1: The Politics of Surveillance Backlash

Early in the pandemic, the aggressive use of intrusive digital (and physical) surveillance by China, South Korea, Israel, and other nations created legitimate fear that governments across the globe might use public health as cover to expand surveillance. But the American public's resistance to surveillance has proved stronger than the government's interest and will to surveil.

Journalists and privacy advocates consistently emphasized the risk of surveillance creep by both government and tech companies seeking to exploit data, but without considering how the public health context might affect privacy trade-offs and without acknowledging the particular privacy protections incorporated into any specific proposal or tool.

Several articles warned that the digital tools in development to combat COVID-19 would have the potential for unchecked expansion of government surveillance.[29] But with only a few notable exceptions, like the first version of North Dakota's rushed Care19 Diary app,[30] the contact-tracing apps that were gaining traction in the United States early in the pandemic were intentionally

[28] Ramesh Raskar et al., "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic," Arxiv, March 19, 2020, https://arxiv.org/pdf/2003.08567.pdf.
[29] See, e.g., Singer and Choe Sang Hun, "As Coronavirus Surveillance Escalates, Personal Privacy Plummets"; Mike Giglio, "Would You Sacrifice Your Privacy to Get Out of Quarantine?" *The Atlantic*, April 22, 2020, www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/.
[30] Jack Morse, "North Dakota Launched a Contact-Tracing App. It's Not Going Well," *Mashable,* May 6, 2020, mashable.com/article/north-dakota-contact-tracing-app/.

designed to guard against unnecessary privacy invasions in direct response to the fear of surveillance creep.[31]

One of the first to gain national attention, the MIT-developed SafePaths app, published an extensive analysis of how the app's proposed combination of GPS-based location information and anonymous Bluetooth-based identifiers would protect user privacy and guard against government surveillance while maximizing the use of data to fight the pandemic.[32] Similarly, an international group of volunteers developed Covid Watch, the first decentralized Bluetooth-based app, specifically to provide an alternative to the intrusive data collection methods used by China and South Korea.[33] The Google-Apple system followed Covid Watch's lead in response to calls by the American Civil Liberties Union and others to limit digital contact-tracing apps to using Bluetooth-based systems to protect user privacy. Indeed, in June the *MIT Technology Review* published an article analyzing how the tool's privacy protections far exceeded those called for in the draft privacy legislation.[34]

In stark contrast to the many other tools that Apple and Google provide and use to collect personal information on users,[35] the Google-Apple system is privacy protective to a fault. The system goes out of its way to avoid collecting any information that could identify a person; gives users complete control over whether, when, and how to share that information; and tightly restricts what public health authorities can do with it.

Yet privacy advocates and the press were unrelenting, and often ignored the extensive protections these apps included. A recent *San Francisco Chronicle* article warned that widespread adoption of the Bluetooth-based Google-Apple system creates "a huge risk that data would live on well beyond the pandemic, giving governments and corporations easy access to information about people's movements and healthcare needs that eclipses what they now have."[36] Public misunderstanding

---

[31] Hannah Murphy, "U.S. and Europe Race to Develop 'Contact Tracing' Apps," *Financial Times*, March 4, 2020.

[32] See Raskar et al., "Apps Gone Rogue."

[33] See Tom Abate, "Stanford Researchers Help Develop Privacy-Focused Coronavirus Alert App," *Stanford News,* April 9, 2020, news.stanford.edu/2020/04/09/stanford-researchers-help-develop-privacy-focused-coronavirus-alert-app/.

[34] Bobbie Johnson, "The US's Draft Law on Contact Tracing Apps Is a Step Behind Google and Apple," *MIT Technology Review*, June 2, 2020, www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/.

[35] Aliza Vigderman & Gabe Turner, "The Data Big Tech Companies Have on You, "Security, Oct. 27, 2020.

[36] Evan Halper, "Lawmakers Warn Coronavirus Contact-Tracing Is Ripe for Abusive Surveillance," *Los Angeles Times*, April 26, 2020, www.latimes.com/politics/story/2020-04-26/privacy-americans-trade-off-trace-coronavirus-contacts.

about the privacy risks of COVID-19 apps is so widespread that articles about *other* surveillance technologies use COVID-19 apps as an unfavorable comparison.[37]

Second, and related, distrust in government generally by both the left and the right escalated quickly during the pandemic, reinforcing the fear of surveillance and abuse of state power. While the concerns differed substantially on each side, they combined to produce a dominant and persistent narrative that contact-tracing apps were dangerous threats to privacy and freedom. Protests against shutdown orders and mask mandates extended to both manual and digital contact tracing. One widely shared Facebook post claimed that a House bill to expand and fund manual contact tracing would "'give the government the power to forcibly remove' children from their homes."[38] An Ohio lawmaker warned constituents that "armies of agents" will be "trained on Apple and Google technology to trace or track people" and will "forcibly isolate" anyone who tests positive and all of their contacts.[39] Unsurprisingly, nearly one-third of public health authorities surveyed by Reuters in early August reported problems with people not answering contact-tracing calls or giving inaccurate information, often objecting that contact tracing invaded their privacy rights.[40]

At the same time, police use of social media and other surveillance tools during the widespread protests against police violence raised fears that traditional contact-tracing tools could be used to track down protestors, a concern made explicit by the Minnesota public safety commissioner's widely reported reference to protest surveillance as "contact tracing."[41]

In addition to mistrust of government surveillance, COVID-19 apps also trigger public distrust in big tech. Indeed, in a survey of public attitudes toward COVID-19 apps, respondents were more distrustful of tech companies than of public health authorities or health insurers. Politicians could

---

[37] Christine Rosen, "The Long, Complicated History of 'People Analytics'," *MIT Technology Review*, Aug. 19, 2020.
[38] Angelo Fichera, "False Claim of Forced Removals Under Contact Tracing Bill," FactCheck.org, May 13, 2020.
[39] Facebook post of Rep. Nino Vitale, May 12, 2020, https://www.facebook.com/RepVitale/posts/2898165580261473.
[40] Benjamin Lesser et al., "Special Report: Local Governments 'Overwhelmed' in Race to Trace U.S. COVID Contacts," Reuters, Aug. 4, 2020, www.reuters.com/article/us-health-coronavirus-tracing-specialrep/special-report-local-governments-overwhelmed-in-race-to-trace-u-s-covid-contacts-idUSKCN2501GK.
[41] Andy Meek, "Minnesota Is Now Using Contact Tracing to Track Protestors, as Demonstrations Escalate," BGR, May 30, 2020, bgr.com/2020/05/30/minnesota-protest-contact-tracing-used-to-track-demonstrators/.

face political backlash for endorsing COVID-19 apps even if the government is completely uninvolved in the data collection and analysis.[42]

As a result, contact-tracing apps quickly became a political nonstarter even before they were available and with no regard to the privacy protections they included. After South Carolina announced plans to become one of only three states to develop an app using the Google-Apple system, lawmakers amended a COVID-19 spending bill to include language banning state agencies from using contact-tracing apps.[43] Kansas passed a similar set of restrictions, and the Ohio House even passed a bill limiting *manual* contact tracing.[44]

To be sure, concerns that government and big tech could use the public health crisis as an excuse to extend citizen and consumer surveillance are understandable and arguably warranted. The United States has had a recent history with the government's rush to develop and deploy surveillance tools after 9/11, and technology companies are in the middle of a public reckoning over their data practices that was years in the making. Since early adopters of digital COVID-19 surveillance tools, such as China and even South Korea, were in fact deploying them without privacy restrictions, and with fluid coordination with law enforcement, Americans were right to demand a different model rather than reflexively following the path of other governments.

But even after it became clear that the models emerging in the United States were highly privacy protective (to a fault, in the case of the Google-Apple system), the privacy critique only intensified in ways that were increasingly detached from the reality of how the tools work.[45] Distrust has crowded out the public conversation so that the United States has not had a chance to honestly and

---

[42] Washington Post–University of Maryland national poll, April 21–26, 2020, *Washington Post*, May 21, 2020, www.washingtonpost.com/context/washington-post-university-of-maryland-national-poll-april-21-26-2020/3583b4e9-66be-4ed6-a457-f6630a550ddf/.

[43] Perera, "South Carolina Legislature Puts Coronavirus Apps on Hold."

[44] Editorial Board, "Worried About COVID-19 Contact Tracing and Privacy? Kansas has the Right Approach," *Kansas City Star*, June 11, 2020, www.kansascity.com/opinion/editorials/article243438946.html; and Karen Kasler, "House Passes Bill Requiring Written Permission for COVID-19 Contact Tracing," WKSU, June 1, 2020, www.wksu.org/health-science/2020-06-01/house-passes-bill-requiring-written-permission-for-covid-19-contact-tracing.

[45] Tiffany C. Li, "Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis," *Loyola University of Chicago Law Journal* 52 (forthcoming 2021) (presuming that contact-tracing apps would not handle and restrict access to data in accordance with their own promises); and Woodrow Hartzog, "Coronavirus Tracing Apps Are Coming. Here's How They Could Reshape Surveillance as We Know It," *Los Angeles Times*, May 12, 2020, www.latimes.com/opinion/story/2020-05-12/coronavirus-tracing-app-apple-google.

dispassionately discuss how privacy expectations should fit in the complex trade-offs being made to protect lives during the pandemic.

Society often does prefer to curtail some liberties to save the lives (and, thus, the liberties) of others. COVID-19 has transformed myriad decisions that normally are the prerogative of each individual into issues that affect our collective health and safety. The usual rules for working, traveling, worshiping, and going about one's day have been upended by the unique and stressful circumstances of managing the virus. Expectations about data privacy also need to undergo an acid wash of scrutiny to make sure that risks are minimized in all of their forms.

Barrier 2: Google and Apple's Public Relations Problems

Already under fire from lawmakers and privacy advocates for their aggressive and well-documented use of personal information, Google and Apple attempted to get ahead of the distrust that was accumulating around digital contact tracing from both the left and the right. The two companies developed a Bluetooth-only technical standard and strict limits on how the apps could collect and share information.

Google and Apple prohibited any other data from being combined with the Google-Apple system and required almost all data to reside on individuals' phones. They also required consent and full user control at every step of the process (including whether and when to report a positive test result to public health authorities). Apps would have to undergo a rigorous approval process before being allowed into the app stores.[46] If the goal is to minimize privacy risks at any cost, then this approach makes a lot of sense. But it has serious downsides for public health.[47]

Before Apple and Google announced their plan, a complex ecosystem of applications with a variety of approaches to protecting user privacy was emerging to assist public health authorities with contact tracing. Rather than spurring that kind of innovation and allowing public health authorities to drive the configuration of these apps, Apple and Google effectively prevented their tool from doing anything other than proximity-based exposure notification. Because these two behemoths together account for nearly 100 percent of the mobile phone operating systems globally, their

---

[46] Etherington, "Apple and Google Release Sample Code."

[47] As Peter Swire put it, the COVID-19 apps that Google and Apple facilitate are a form of "public health theater. Peter Swire, "Security, Privacy and the Coronavirus: Lessons From 9/11," *Lawfare,* March 24, 2020, www.lawfareblog.com/security-privacy-and-coronavirus-lessons-911. Bruce Schneier, whom Swire credits for the concept, made one of the strongest cases that the limitations of Bluetooth technology will result in apps that produce unacceptable numbers of false positives and false negatives. Bruce Schneier, "Me on COVID-19 Contact Tracing Apps," Schneier on Security, May 5, 2020, www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html.

decision to impose a decentralized, Bluetooth-only model short-circuited a more thorough debate about how to balance privacy against everything else that's valued.[48] Their inflexible position completely shut down the rapidly emerging ecosystem of apps that offered alternative models for balancing privacy and efficacy, including several that the governments of Germany, France, and the United Kingdom were developing.[49] These apps and others would have combined more data or adopted a transparent centralized model while still providing significant levels of privacy.[50]

The constraints created by the tech giants severely limit the apps' potential to help track and trace new potential cases. The information the apps collect can't be used by manual contact tracers either to identify potential new cases or augment a person's memory. Instead, Apple and Google have created an entirely separate system that, at best, can work in parallel with traditional contact tracing.[51]

Realizing even that limited promise requires a significant number of people to download and start running the app on a regular basis. Early research on Bluetooth-only models suggested that close to 60 percent of smartphone users would need to use an app to substantially reduce the spread of the

[48] See Tom Loosemore, "Google and Apple's Diktat to Governments on Coronavirus Contact-Tracing Apps Is a Troubling Display of Unaccountable Power," *Business Insider*, June 24, 2020; and Shannon Bond, "Apple, Google Coronavirus Tool Won't Track Your Location. That Worries Some States," NPR, May 13, 2020, www.npr.org/2020/05/13/855064165/apple-google-coronavirus-tech-wont-track-your-location-that-worries-some-states.

[49] See Alex Webb, "Apple and Google Face Off Against Europe Over Contact Tracing," *Bloomberg Business Week*, May 18, 2020, www.bloomberg.com/news/articles/2020-05-18/apple-and-google-face-off-against-europe-over-contact-tracing; Douglas Busvine & Andreas Rinke, "Germany Flips to Apple-Google Approach on Smartphone Contact Tracing," Reuters, April 26, 2020, www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J; and Kelion, "Coronavirus: Apple and France in Stand-Off Over Contact-Tracing App," BBC, April 21, 2020, https://www.bbc.com/news/technology-52366129.

[50] See Ieva Ilves, "Why Are Google and Apple Dictating How European Democracies Fight Coronavirus?" *The Guardian*, June 16, 2020, https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus; Raskar et al., "Apps Gone Rogue" (describing the SafePaths app privacy protections). The centralized databases several of these used also would have provided the information necessary to determine whether the apps were working, which is impossible under the decentralized systems Google and Apple have mandated. See Rory Cellan-Jones & Leo Kelion, "Coronavirus: The Great Contact-Tracing Apps Mystery," BBC, July 21, 2020, https://www.bbc.com/news/technology-53485569.

[51] See Loosemore, "Google and Apple's Diktat to Governments on Coronavirus Contact-Tracing Apps."

virus, although lower rates could have some impact.[52] A more recent study of the Google-Apple system suggests that it could contribute to modest reductions in infections with adoption rates as low as 15 percent in conjunction with a robust manual contact-tracing system.[53] But five weeks after Maryland launched the first Google-Apple-based app, health officials estimated that it hadn't reached even that low threshold.[54]

There is a certain irony in this. Google and Apple are companies long criticized for knowing "everything" about us.[55] Google Maps alone collects real-time location data of more than one billion people across the world, and Apple permits consumer applications to vacuum up a dizzying range of sensitive personal data even while we're sleeping and location data even when we've turned off location services.[56] Yet the companies have used a much stricter set of privacy controls on a tool to fight the largest public health crisis in more than a generation than they do on run-of-the-mill consumer apps.

Barrier 3: De Facto Immunity for Retailers, Employers, Schools, and Other Landowners

All employers have a general duty to protect their employees from unjustified risks to their health at the workplace, and Occupational Safety and Health Administration (OSHA) guidance makes clear

---

[52] Patrick Howell Neill, "No, Coronavirus Apps Don't Need 60% Adoption to Be Effective," *MIT Technology Review,* June 5, 2020, www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.

[53] Matthew Abueg et al., "Modeling the Combined Effect of Digital Exposure Notification and Non-pharmaceutical Interventions on the COVID-19 Epidemic in Washington State," MedRXiv, Sept. 2, 2020, www.medrxiv.org/content/10.1101/2020.08.29.20184135v1.

[54] Marie Albiges, "About 11% of Virginians With Smartphones Have Downloaded the COVIDWISE App, Northam Says, *The Virginia Pilot,* September 1, 2020, www.pilotonline.com/coronavirus/vp-nw-coronavirus-covidwise-app-downloads-20200901-44uvaub7vzh7vlntjtoayo5bj4-story.html.

[55] See Thomas Tamblyn, "Google Knows Literally Everything About You – Here's How to Delete That Data," *Huffington Post,* March 28, 2018, https://www.huffingtonpost.co.uk/entry/google-knows-literally-everything-about-you-heres-how-to-stop-it_uk_5abb68dde4b06409775b7d2b; Julia Anglin & Jennifer Valentino-Devries, "Apple, Google Collect User Data," *Wall Street Journal*, April 22, 2011, www.wsj.com/articles/SB10001424052748703983704576277101723453610.

[56] See Dale Smith, "*Google Collects a Frightening Amount of Data About You. You Can Find and Delete It Now*, C|Net, June 28, 2020, www.cnet.com/how-to/google-collects-a-frightening-amount-of-data-about-you-you-can-find-and-delete-it-now/; Jeffrey Fowler, "It's the Middle of the Night. Do You Know Who Your iPhone Is Talking To?" *Washington Post,* May 28, 2019, www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/; and Ryan Whitwam, "The iPhone Collects Location Data Even When You Tell It to Stop," Extreme Tech, Dec. 4, 2019, www.extremetech.com/mobile/302996-the-iphone-collects-location-data-even-when-you-tell-it-to-stop.

that COVID-19 is no exception. Indeed, by requiring employers to make reasonable efforts to identify and isolate employees who may have come into contact with a confirmed COVID-19 case, the OSHA guidance issued earlier this year seemed to presage the mass adoption of COVID-19 apps by instructing employers to develop procedures for the prompt identification and isolation of potentially infectious people.[57] Given that employees at retailers are at risk from patrons as well as other employees, it was foreseeable in the spring of 2020 that potential regulatory or civil liability risk could push a few influential firms to adopt and mandate the use of COVID-19 apps, possibly even among customers. This would have started a salutary trend. Although a couple business-to-business firms have experimented with apps, no national chain has been willing to invest in this particular sort of pandemic response.[58] Why not?

For one thing, the prospect of requiring (or even encouraging) app adoption is fraught with public relations danger (see Barriers 1 and 2). Many of the same political problems that a lawmaker would face for encouraging or imposing a tracking technology on constituents are replicated as PR problems for private firms. Companies do not want to force their customers or even their employees to use an app that is perceived to be an invasion of privacy. Even universities, which have a quasi-parental relationship with their "customers," were accused of "abusing" their power by even considering a COVID-19 app mandate.[59] Employment law experts also advised against using apps because of the complicated implications for compliance with privacy or anti-discrimination laws.[60]

Meanwhile, what little concern there may have been about liability risk for *not* adopting an app has evaporated. First, some states, such as Ohio, have passed legislation immunizing businesses from tort liability for all but reckless or intentional COVID-19 infections, and several state attorneys general have been urging Congress to do the same.[61]

---

[57] Occupational Safety and Health Administration, *Guidance on Preparing Workplaces for COVID-19* (OSHA 3990-03 2020), March 2020, www.osha.gov/Publications/OSHA3990.pdf.
[58] Shannon Bond, "Your Boss May Soon Track You at Work for Coronavirus Safety," NPR, May 8, 2020, www.npr.org/2020/05/08/852896051/your-boss-may-soon-track-you-at-work-for-coronavirus-safety.
[59] Gennie Gebhart et al., "University App Mandates Are the Wrong Call," Electronic Frontier Foundation, July 30, 2020, www.eff.org/deeplinks/2020/07/university-app-mandates-are-wrong-call.
[60] "Going Back to Work: Employer Use of 'Apps' on Employee PDAs/Smart Phones for COVID-19 Contact Tracing," Ropes & Gray, May 1, 2020, www.ropesgray.com/en/newsroom/alerts/2020/05/Going-Back-to-Work-Employer-Use-of-Apps-on-Employee-PDAs-Smart-Phones-for-COVID-19-Contact-Tracing.
[61] Patricia Anderson Pryor & Allesandro Botta Blondet, "Ohio Halts COVID-19 Litigation, Providing Civil Immunity for Healthcare, Businesses, and Others," Jackson Lewis, Sept. 14, 2020, www.jacksonlewis.com/publication/ohio-halts-covid-19-litigation-providing-civil-immunity-healthcare-businesses-and-others; and "State Attorneys General on SAFE TO WORK Act Liability

Even without formal immunity, tort liability based on a theory of preventable exposure has been difficult for plaintiffs, even under the best of circumstances. As Josh Czaczkes, Tom Baker, and John Fabian Witt explain,

> "An important starting point is to observe just how difficult winning COVID-19 liability cases will be. Plaintiffs will need to show that defendants owed them a duty of care and to prove that such defendants behaved negligently around some COVID-19 risk. Defendants who follow the prevailing norms of their industry or field will be able to offer that fact as a consideration in their favor. Even where a plaintiff can successfully show negligence, the plaintiff will still need to prove that it is more likely than not that absent the defendant's negligence the plaintiff would not have gotten sick. And last, as a practical matter, a plaintiff will need to be able to prove damages sufficient to make a lawsuit worthwhile. Only the sickest COVID-19 patients or their estates will satisfy this last criterion, and few plaintiffs will be able to make all these showings."[62]

However, some plaintiffs will be able to prove that they contracted the coronavirus from a person who was granted entry to a store or place of business even though they either had a confirmed case of COVID-19 or had been in direct and sustained contact with such a person. This is the sort of exposure that a well-functioning COVID-19 app could greatly reduce.

In theory, business insurance companies (which by and large cover COVID-19-related claims) should put pressure on industry to use the best available tools to reduce risk anyway since the liability risk in the aggregate, across hundreds of covered firms, may be nontrivial. But there is a widespread informal understanding among insurance companies that if a business adheres to the guidelines maintained by the CDC and the local public health authority, it will be considered to have acted reasonably.[63] The Safe to Work Act introduced in the Senate would create a safe harbor

---

Protections," Aug. 5, 2020, https://law.georgia.gov/document/document/ltrtocongressinsupportofsafetoworkact22statesignaturespdf/download.

[62] Josch Czaczkes et al., "Why We Don't Need COVID-19 Immunity Legislation," Balkinization, Sept. 26, 2020, balkin.blogspot.com/2020/09/why-we-dont-need-covid-19-immunity.html.

[63] See Advisory Board, "The First Wave of Covid-19 Workplace Lawsuits Is Here," Daily Briefing, Aug. 3, 2020, www.advisory.com/daily-briefing/2020/08/03/covid-lawsuits; Jessica Ragosta Early et al., "COVID-19 Civil Immunity Under Proposed Federal SAFE TO WORK Act and State Laws," Holland & Knight Alert, Aug. 13, 2020, www.hklaw.com/en/insights/publications/2020/08/covid19-civil-immunity-under-proposed-federal-safe-to-work-act.

on this basis.[64] (Ronen Perry suggests that even noncompliance with CDC standards might not constitute a breach of care under difficult circumstances like pandemic management.[65])

Since none of the public health guidance documents advocate for the use of apps or other surveillance tech, courts are unlikely to find that any firm was unreasonable for failing to force employees or customers to use a COVID-19 app. Thus, insurers have not and will not force landowners or businesses to use apps.

Ironically, if COVID-19 apps made a nontrivial contribution to pandemic management, they could make it easier for a plaintiff to prove causation in negligent exposure cases. If we were cynical, we might think there is a *disincentive* among insurance companies—which would have to pay out COVID-19 litigation losses—to recommend or require the adoption of these technologies, *especially* if they help track preventable infections.

In any case, de facto tort immunity removes the incentive and the excuse for companies to force entrants or employees to use an app. But in fairness, it's hard to blame the private sector: If the CDC and state public health authorities are not willing to endorse even the concept of a COVID-19 app (let alone recommend adoption), then legislators and courts are unlikely to treat apps as a necessary part of responsible pandemic management.

Barrier 4: Lost Interest Among the General Public

Initially, the general public was receptive to apps that might help manage the crisis. Americans seemed to understand the trade-offs and approve of automatic data collection. A study released in May 2020 by University of Washington researchers found that most Americans felt neutrally or positively about the prospect of sharing location data with the government for the purposes of pandemic management.[66] A Pew Research Center report around the same time found that Black and Hispanic Americans, who typically have higher levels of distrust for the government and privacy-invasive technology, were notably *more* likely to say that it is acceptable for the government to

[64] Safe to Work Act, S. 4317 116th Congress (2020), www.congress.gov/bill/116th-congress/senate-bill/4317/text#toc-id368E3064D88542E7A1FDE5C618B58155.
[65] Ronen Perry, "Who Should Be Liable for the COVID-19 Pandemic?" *Harvard Journal on Legislation* (forthcoming 2020), papers.ssrn.com/sol3/papers.cfm?abstract_id=3697283.
[66] Simko et al., "COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences," May 8, 2020, https://seclab.cs.washington.edu/wp-content/uploads/2020/05/contact-tracing-user-privacy.pdf.

track cell phones as part of the pandemic response.[67] (This finding could well be explained by heightened risk of having severe complications from the virus among minority communities.)

These empirical findings suggest that the general reluctance to embrace COVID-19 apps has had winners and losers. While some people prefer the freedom from pressure to adopt a new surveillance tool, others might experience more freedom from being able to resume normal activities more safely with the help of an app.

However, negative reactions are much more likely to be expressed by individuals who disfavor an app than by those who favor them. There are no direct and felt consequences from the government's *failure* to develop apps; there are only indirect and diffuse harms from not doing as much as it could. Of all the things that the government *could* have done better, promoting digital COVID-19 apps is low on the list, in part because the gains are unclear and unfamiliar.

It's also possible that there would have been public pressure to use all possible tools, including tracking apps, if the mortality risks from the disease were higher. To be sure, the COVID-19 crisis *is* the worst threat from contagious disease that the United States has faced in more than a century, but it's not as deadly as it seemed initially. In March, the World Health Organization had estimated that the case fatality rate was 3–4 percent.[68] These estimates, derived by dividing the number of COVID-19-related deaths by the number of confirmed cases, greatly undercounted the actual number of cases (and thus overestimated the death rate). Early estimates of case fatality rates were also biased because, in many regions hit hardest early in the pandemic, the infected population was disproportionately elderly. Today, the CDC estimates that the infection fatality rate is much lower for the general population, and less than 0.02 percent for individuals under age fifty.[69] These estimates are consistent with data coming from other countries where the virus ripped through communities mostly unabated by public health interventions.[70] This means that many Americans

---

[67] Monica Anderson & Brooke Auxier, "Most Americans Don't Think Cellphone Tracking Will Help Limit COVID-19, Are Divided on Whether It's Acceptable," Pew Research Center, April 16, 2020, www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable/.

[68] World Health Organization, "Coronavirus Disease (COVID-19): Similarities and Differences With Influenza," March 17, 2020, www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-similarities-and-differences-covid-19-and-influenza.

[69] Centers for Disease Control and Prevention, "COVID-19 Pandemic Planning Scenarios," www.cdc.gov/coronavirus/2019-ncov/hcp/planning-scenarios.html#table-1 (last visited Oct. 29, 2020).

[70] Axel Lexmond et al., "Evolution of COVID-19 Cases in Selected Low- and Middle-Income Countries: Have They Peaked Due to High Levels of Infection and Immunity?" MedRXiv, Sept. 26, 2020, www.medrxiv.org/content/10.1101/2020.09.26.20201814v1

have felt safe returning to semi-normal social behavior without tech-assisted safeguards, with the predictable result of another massive surge in cases and rumblings of imminent shutdowns.[71]

Finally, the public has been told repeatedly that apps are privacy invasive and don't work. Many critics, including Bruce Schneier and others, have argued that apps are futile.[72] To a large extent, this public commentary attacks a straw man argument that COVID-19 apps would solve the crisis alone and does not seriously and carefully consider how communications technologies could be part of an interlocking set of tools.[73] In fact, new modeling suggests that even low levels of exposure notification app adoption (15 percent) could reduce the death rate by more than 6 percent.[74] Indeed, app critics often characterized even the privacy-to-a-fault Google-Apple system as an invasive data grab by big tech, creating the false impression that COVID-19 apps, regardless of design, pose new and unusual privacy and security risks without comparing the apps to the sorts of commercial apps that collect location data and are in routine use.[75]

If the public is consistently told that COVID-19 apps are dangerous and don't work, and nobody is using them anyhow, there's little reason to expect a public pressure campaign.

LESSONS FOR NEXT TIME AROUND

An effective test-and-trace system doesn't have to give up on privacy. It only requires considering privacy in the broader context of the dire public health emergency the United States is facing and in light of the other substantial compromises being made to address it. Most of the privacy concerns around digital contact tracing could be guarded against as well or even better by strong, verifiable, and enforceable restrictions on how every person's data is accessed, used, stored, and deleted. In

[71] See Andrew Joseph, "'At a Breaking Point': New Surge of Covid-19 Cases Has States, Hospitals Scrambling, Yet Again," STAT, Oct. 20, 2020, www.statnews.com/2020/10/20/at-a-breaking-point-new-surge-of-covid-19-cases-has-states-hospitals-scrambling-yet-again/; "See How All 50 States Are Reopening (and Closing Again)," *New York Times*, www.nytimes.com/interactive/2020/us/states-reopen-map-coronavirus.html (visited on Nov. 9, 2020).
[72] See Schneier, "Me on COVID-19 Contact Tracing Apps"; Soltani et al., "Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis."
[73] See, e.g., Simko et al., "COVID-19 Contact Tracing and Privacy."
[74] See Abueg et al., "Modeling the Combined Effect of Digital Exposure Notification and Non-pharmaceutical Interventions on the COVID-19 Epidemic in Washington State."
[75] See Brandon Vigliarolo, "Over 75% of Android Apps Are Secretly Tracking Users," Tech Republic, Nov. 29, 2017, www.techrepublic.com/article/over-75-of-android-apps-are-secretly-tracking-users/.

other words, it's possible to protect privacy without hamstringing a potentially critical tool to manage the pandemic.

The law already recognizes this fact. For decades, common law rules and privacy laws have treated communicable disease as a special circumstance that justifies entrusting health authorities with rights to use sensitive data to protect the public. Recent COVID-19-related HIPAA (Health Insurance Portability and Accountability Act) guidance notes that the law's otherwise strict consent requirement doesn't apply to sharing otherwise private information with public health authorities to protect public health and treat individual patients.[76]

Likewise, state laws often affirmatively require doctors and patients to disclose the risk of communicable disease to others whom they may have infected. New York, for example, requires doctors to report the relevant contacts of their patients who have tested positive for HIV to public health authorities and to notify patients' past partners about the risks if the patients do not do so themselves.[77]

Even the General Data Protection Regulation (GDPR), Europe's strict privacy law, allows for the collection and processing of data without consent in the context of a public health emergency.[78] (Largely due to the same misplaced distrust of surveillance creep, the European Commission has opted to advise member states not to use this exception, insisting that users must opt in to any automatic data collection for pandemic management.[79])

Lesson 1: Socially Responsible Privacy Trade-Offs

American policy experts assume, and the European Commission has expressly required, that digital contact tracing should incorporate far more stringent privacy protections than are normally imposed

[76] U.S. Department of Health and Human Services, Office for Civil Rights, "BULLETIN: HIPAA Privacy and Novel Coronavirus," February 2020, www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.
[77] New York State Department of Health, "HIV Reporting and Partner Notification Questions and Answers," https://www.health.ny.gov/diseases/aids/providers/regulations/reporting_and_notification/question_answer.htm#fiftyfive (last visited Oct. 29, 2020).
[78] General Data Protection Regulation, Article 6, Recital 46, https://gdpr-info.eu/art-6-gdpr/.
[79] eHealth Network, "Mobile Applications to Support Contact Tracing in the EU's Fight Against COVID-19: Common EU Toolbox for Member States," Version 1.0, April 15, 2020, ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

on data collection methods for public health purposes, including manual contact tracing.[80] In some sense, this is rational since the risk from large troves of data, collected inexpensively and frictionlessly, are different from the risks of painstaking collections of manual tracing data. But during a pandemic, the heightened requirements make much less sense—particularly when *other* forms of privacy protection can be put in place.

Moreover, a pandemic pushes privacy into conflict with health and other liberties. Consider the following hypothetical: Alice, Bill, and Chris have downloaded their state's COVID-19 tracking app, which uses the Google-Apple system. Chris can work from home and, because he has a preexisting health condition, he is reluctant to leave his house unless he has confidence that the risk of viral spread is well managed.

David and Elise each have contracted the virus but have no symptoms and are unaware they are infected. They have been near Alice and Bill, respectively, in an indoor environment. The next day, they develop symptoms and get tested for the coronavirus. Both tests come back positive. Because David never downloaded the COVID-19 app, neither he nor the public health authorities have a record of his contact with Alice. Thus, he had no way of communicating his test status to her or to others who came in close contact with him.

Elise *has* downloaded the app and dutifully reports her positive test result through the app. Bill notices the exposure notification, but all he knows is that somebody he saw yesterday has tested positive. Because Bill was at an outdoor event yesterday, he is not sure whether to take the alert seriously. Missing a week of work would be a hardship, so he decides to continue to go to work and other public places rather than quarantining.

What happened to Chris? He has decided to continue to shelter in place and avoid contact with his family and friends because he rightly infers that people have no reliable way of evaluating their risk of exposure.[81] Thus, the privacy decisions of David and of Apple and Google have consequences for the health and liberty of Alice, Bill, and Chris.

This example illustrates why it doesn't make sense to impose a rigid privacy model that precludes some modest privacy trade-offs to help save lives and safely reopen the economy. Lockdowns sacrifice liberty and economic security to protect health in substantial ways. Privacy should be no

---

[80] See eHealth Network, "Mobile Applications to Support Contact Tracing in the EU's Fight Against COVID-19; Paul Schwartz, "Protecting Privacy on COVID-19 Surveillance Apps," IAPP, May 8, 2020, iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps/.

[81] Steven Goodreau et al. on behalf of the Statnet Development Team, "Can't I Please Visit Just One Friend? *Visualizing Social Distancing Networks in the Era of COVID-19*," statnet.org/COVID-JustOneFriend/ (last visited Nov. 9, 2020).

different. To quote one employee of the Electronic Privacy Information Center (EPIC), a preeminent privacy advocacy organization, responding to the risks of COVID-19, "privacy is something that's constantly weighed against other things."[82]

Privacy depends on context. Here that context is a public health emergency triggered by a deadly, highly infectious, new disease with characteristics that make traditional contact-tracing methods unlikely to work well. Properly configured COVID-19 apps provide a new tool to make manual contact tracing more effective simply by automating and expanding the collection of the same information *we already collect* through that widely accepted process. If we accept—as we have for hundreds of years—that contact tracers should collect location data from people who contract the coronavirus, then it makes little sense to say that they should be banned from even asking people to use an app to do the same thing.

The scale of data collection seems to drive a lot of the concern. Yet there's a marked absence of outrage over new digital tools that private companies like Salesforce.com have developed to streamline manual contact tracing to improve speed and accuracy, even though they automate the collection of personal information in ways that largely mirror digital contact-tracing apps.[83] By contrast, the discussion of more automated (and, thus, larger scale) contact-tracing apps largely starts and ends with privacy. Many commentators, including technologists, are still unwilling to think through socially responsible trade-offs among privacy, human life, other liberties, and economic costs.[84] Instead, the prevailing wisdom argues that GPS-location data should be off the table "without discussion," as one prominent group of academics put it.[85]

Something is very wrong with the discourse about privacy in this context. COVID-19 apps have been disfigured by policies that assume worst-case scenarios for privacy risk, and that prematurely and dramatically discount their potential benefits. Thus, one overarching lesson is that privacy

---

[82] Issie Lapowski, "EPIC Is in Turmoil After Its President Took a Coronavirus Test Without Telling Staff. It Came Back Positive," Protocol, April 16, 2020, www.protocol.com/epic-president-coronavirus-marc-rotenberg.

[83] Karen Verspoerd & Nick Geard, "Victoria's Coronavirus Contact Tracing Is About to Get Faster. Let's Make It the First Step in a Larger Digital Boost," The Conversation, Sept. 10, 2020, theconversation.com/victorias-coronavirus-contact-tracing-is-about-to-get-faster-lets-make-it-the-first-step-in-a-larger-digital-boost-145759; and Salesforce.com, "Contact Tracing," www.salesforcepublicsectordemos.com/tours/contact-tracing.

[84] Association for Computing Machinery Europe Technology Policy Committee, "Statement on Essential Principles and Practices for COVID-19 Contact Tracing Applications," May 5, 2020, www.acm.org/binaries/content/assets/public-policy/europe-tpc-contact-tracing-statement.pdf.

[85] Dali Kafaar et al., "Joint Statement on Contact Tracing: Date 19th April 2020," April 19, 2020, https://giuper.github.io/JointStatement.pdf.

should be discussed in a more context-dependent way, with a problem-solving orientation rather than with rhetoric that ratchets up the sense of threat and entitlement. Disease surveillance has risks, to be sure, but it also has benefits. A National Bureau of Economic Research study shows the cost of unjustified paralysis: South Korea saved about seven thousand lives by disclosing the location histories of everybody who tested positive for the coronavirus.[86] An ethical discussion of COVID-19 app privacy should start with the expectation that the app should optimize for saving lives within reasonable bounds of privacy risk.

Lesson 2: Trustworthy Health Surveillance Systems

The starting point for any trustworthy data surveillance program is that it must be designed and used solely for public health, and it must work well enough to justify the privacy and other costs it creates.

A trustworthy data surveillance system will keep sensitive health data secure from redistribution or repurposing and will consistently assess whether there is sufficient efficacy to continue the program. Thus, at the start, a trustworthy environment for emerging disease surveillance technologies requires credible privacy commitments.

Even in an era of government distrust, privacy rules can be clear, and compliance can be verified. Disease surveillance is very different from counterterrorism. The legitimate need to hide sources and methods makes meaningful transparency and effective oversight of national security surveillance programs impossible. For counterterrorism, we must have faith in the checking function of secret courts that oversee intelligence surveillance, and there is no terminal event or obvious stopping point for the threat to national security.

The pandemic is different. Surveillance programs can be monitored and audited, without disclosing personally identifying information, to ensure compliance with data access and purpose limitations.

Finally, in addition to efficacy and privacy, trustworthiness requires regular assessments to make sure these tools are improving our ability to track and trace the virus and are safe from abuse. (This should include monitoring whether, instead of freeing up resources to focus manual contact tracing and other measures on high-risk communities, these tools exacerbate inequalities by driving away resources from those efforts.)

---

[86] David Argente et al., "The Cost of Privacy: Welfare Effects of the Disclosure of COVID-19 Cases" (National Bureau of Economic Research Working Paper No. 27220), May 2020, www.nber.org/papers/w27220.pdf.

Lesson 3: Dormant Pandemic Law

Some of the barriers to effective technology-assisted disease surveillance are rooted deeply enough in American political culture that they are likely to arise in future pandemics. When disaster has let up, and Congress sets up a commission to reflect on governmental failures during the COVID-19 crisis, policymakers would do well to set up a modern slate of emergency laws that are activated automatically when certain emergency conditions are met (for example, when the World Health Organization declares a pandemic). Laws that enable the responsible use of surveillance technologies during an epidemic would be particularly valuable not only to save valuable time but also to insulate future political actors from short-term negative public reactions.

When equipped with tools that can help reduce both infection rates *and* quarantines, and with strong privacy rules already in place, public health experts would be much more likely to experiment with tracking technologies and, if they prove efficacious, to strongly recommend them.

The essential elements of a pandemic data surveillance scheme mirror the efficacy and privacy principles we described at the beginning of this paper:[87]

- **Springing Data Repository.** When the CDC officially recognizes a pandemic, a set of legal rules should become activated automatically to allow for effective surveillance. The CDC should be authorized to create and administer a data repository, and to develop a data collection program that draws on the function and affordances of available commercial technologies. The data repository should be maintained in a way that state and local public health authorities can access it to deposit testing data, generate risk scores, and communicate information or instructions to individuals. Authorization to create the data repository should be paired with a requirement that a congressional subcommittee or an independent oversight board monitors the administration of a data surveillance program.
- **Access Limitations.** Data should be accessed only by public health authorities and by companies whose participation is needed for functionality. Data should be accessed only for a narrow set of purposes related directly to controlling the spread of disease, and raw data may not be redisclosed. Law enforcement use of the data should be explicitly prohibited.
- **Transparency by Design.** Every aspect of the system specifications (but not the user data) should be open to public scrutiny. All software should use open source code so that its functioning can be understood and no features can be hidden, all access to the data

[87] For a much richer analysis of the policy standards that should apply to digital disease surveillance (with conclusions congruent to our own), see Alan Z. Rozenshtein, "Digital Disease Surveillance," *American University Law Review* 70 (forthcoming 2021).

repository should be logged, and the access logs should be publicly accessible. The purpose of any nonroutine access should also be logged.

- **Automatic Sunset.** Perhaps the most important privacy protection is to ensure that the data repository lasts only as long as the need for the program. The program should expire automatically when the emergency has ended or when an internal or independent review finds that the data surveillance has not added sufficient value for controlling the outbreak.[88]

A bipartisan group of legislators attempted to create data governance ground rules in the Exposure Notification Privacy Act (ENPA), and leading privacy advocates recently urged California lawmakers to adopt similar contact-tracing privacy principles. We take issue with the particular policies embraced by these proposals, but the general concept of a context-specific background privacy law is sound. Privacy laws can allow responsible apps to flourish.[89]

Unfortunately, the specific policy proposals embodied in draft legislation like ENPA tend to validate and further entrench many of the barriers we have identified rather than overcome them. For example, current proposals place a high standard for acceptable user consent. ENPA would have prohibited public health authorities from requiring apps as a condition for reopening generally and even prevented individual private businesses from choosing to require participation in a COVID-19 app program.[90] But public health authorities should have the authority to recognize app use as an appropriate alternative to broad quarantines. After all, use of an app can be seen as the less coercive alternative to the ample options that federal and state laws give health authorities when they are combating the spread of infectious diseases, such as quarantines and lockdowns.[91] Private venues

---

[88] Note that, although efficacy is important, any new disease surveillance program needs time to work. Novel technologies typically have a learning curve and improve with use. Even the Google-Apple system, with all its limitations, is showing more promise than many (including we) originally predicted. See Kif Leswing, "States Are Finally Starting to Use the Covid-Tracking Tech Apple and Google Built — Here's Why," CNBC, Oct. 3, 2020, www.cnbc.com/2020/10/03/covid-app-exposure-notification-apple-google.html.

[89] Exposure Notification Privacy Act, S. 3861, 116th Congress (2020), www.congress.gov/bill/116th-congress/senate-bill/3861; and ACLU of California, et. al., "2020-08 Coalition Letter to Governor/Legislature on Contact Tracing and Privacy," August 2020, https://www.eff.org/DOCUMENT/2020-08-COALITION-LETTER-GOVERNORLEGISLATURE-CONTACT-TRACING-AND-PRIVACY.

[90] See Exposure Notification Privacy Act, § 8.

[91] See Centers for Disease Control and Prevention, "Specific Laws and Regulations Governing the Control of Communicable Diseases," www.cdc.gov/quarantine/specificlawsregulations.html; National

and businesses, too, should be under some pressure to ensure that patrons and employees take appropriate precautions, like wearing masks.

Another problem with ENPA is that it embraced the idea that data should be decentralized rather than collected and stored by public health authorities. This underestimates the value in centralized data collections, which allow for better assessments of risk. Moreover, state laws *already* require that testing and health care facilities report new cases of communicable diseases, including COVID-19, directly to public health authorities. Centralized data is an inevitable part of pandemic management: Some diseases are too dangerous to let each person decide whether and when to let close contacts know they might have been infected. Forcing individual users to take responsibility for the process also makes the process error-prone and inefficient.

Although the current proposals are flawed, it is heartening to see Congress and state legislatures recognize the need for forward-looking pandemic legislation. We hope this work will continue.

CONCLUSION

A soccer player at a high school in Ohio came down with COVID-19 symptoms on a recent Saturday, the day the team played against a cross-town rival. The school's athletic director called an emergency Zoom meeting that evening with the coach, the bus driver, the principal, and the player's four teachers to figure out who might have been exposed. CDC guidelines advise that the entire team should quarantine in situations like this *if they had been in close contact with the athlete*.[92] Updated guidance defines "close contact" as having been within six feet of an infected person for a *cumulative* total of fifteen minutes or more over any single twenty-four-hour period in the two days before symptoms appeared and regardless of whether the contacts were wearing masks.[93]

How do you make that call? Who was close to the player during practice on Friday? What about at school? Did she walk home with anyone? Who sat next to her on the bus? How close did the players sit on the bench? Since the group couldn't answer these questions, they decided the whole team and the students who sat next to the player in class should self-isolate.

Conference of State Legislatures, "State Quarantine and Isolation Statutes," www.ncsl.org/research/health/state-quarantine-and-isolation-statutes.aspx.

[92] Centers for Disease Control and Prevention, "Youth Sports Program FAQs," June 23, 2020, www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/youth-sports-faq.html.

[93] Centers for Disease Control and Prevention, "Public Health Recommendations," Oct. 21, 2020, www.cdc.gov/coronavirus/2019-ncov/php/public-health-recommendations.html.

Three days later, the player's test came back positive. By that time, she remembered that she had stopped at the local Starbucks to grab a Frappuccino with two other friends on her way home from school on Friday. They waited in line at least 15 minutes and sat together maskless for around an hour. She didn't know how many others were in the store. The tables were at least six feet apart and the line had markers, but people weren't paying close attention.

Repeated across the country, this scenario and variations on it demonstrate why effective COVID-19 apps should play a role in the complex balance between risk avoidance and living somewhat normal lives.

In the teeth of the most significant public health crisis in more than a generation, it's dumbfounding that policymakers and members of the public are suddenly unwilling to trust public health authorities to responsibly collect and use critical information for stopping the spread of a deadly and highly infectious virus. But as case numbers and hospitalizations rise again across the United States, failure even to attempt to develop and deploy COVID-19 apps is leading to more of the bad: more isolation, more death.

The Digital Social Contract paper series is supported by funding from Facebook, which played no role in the selection of the specific topics or authors and which played no editorial role in the individual papers.