Jane Bambauer
Professor of Law
University of Arizona
janebambauer@email.arizona.edu

Brian Ray
Leon M. and Gloria Plevin Professor of Law
Cleveland-Marshall College of Law
b.e.ray@csuohio.edu

Early in the pandemic the aggressive use of extensive—and unnecessarily intrusive—digital (and physical) surveillance by China, South Korea and others created legitimate fear that governments across the globe might use public health as cover to expand surveillance in similar ways that national security was used after 9/11. But in the U.S. at least, those fears so far have proven completely unfounded. Indeed, states and the federal government generally have actively distanced themselves from digital contact tracing.

Why this reluctance? First, journalists and privacy advocates consistently emphasized the risk of surveillance creep both by government and tech companies seeking to exploit data without considering how the public-health context might affect privacy tradeoffs or acknowledging the actual privacy protections these tools include.

"As Coronavirus Surveillance Escalates, Personal Privacy Plummets," was just one of several articles that warned the digital tools governments around the world were using to combat Covid-19 risked unchecked expansion of government surveillance. Similarly, a recent article describing the proliferation of workplace surveillance technologies with the Orwellian name "people analytics" casually associated them with covid-19 tracing applications.

Most commentary on digital contact tracing consistently features these twin tropes of surveillance creep by government and data grabs by tech companies in spite of the fact that, the contact tracing apps that were gaining traction in the U.S. early in the pandemic were built to protect privacy in direct response to the fear of surveillance creep.

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. 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.

Yet press accounts, in particular, often simply ignore the extensive protections these apps include in favor of repeating the dominant surveillance narrative. For example, a recent San Francisco Chronicle article warned that widespread adoption of the Google-Apple exposure notification or "GAEN" 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." But the GAEN 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 restricts what public health authorities can do with that information.

Second, distrust in government by both the left and right quickly escalated during the pandemic Protests against shutdown orders extended to both manual and digital contact tracing. One widely shared Facebook post claimed that a contact tracing funding bill would "give the government the power to forcibly remove" children. An Ohio lawmaker warned constituents that “armies of agents” will be “trained on Apple and Google technology to trace or track people” and “forcibly isolate” them.

At the same time, use of surveillance tools during the widespread protests against police violence raised fears that traditional contact tracing tools could be used to track down protestors, a possibility made explicit by the Minnesota Public Safety Commissioner’s widely reported conflation of protest surveillance and contact tracing.

Tracing apps quickly became a political non-starter even before they were available and with no regard to the privacy protections they included.

Especially early in the pandemic, concerns that big government and big tech would use the public health crisis as an excuse to extend citizen and consumer surveillance clearly were warranted given the U.S. government’s rush to develop and deploy surveillance tools after 9/11 and big tech’s miserable record on protecting personal privacy. To make matters worse, early adopters like China and even South Korea were deploying them as part of extensive surveillance networks.

But, even after it became clear that the models emerging in the U.S. were highly privacy protective, the privacy critique only intensified in ways that were increasingly detached from the reality of how these tools work and without meaningfully analyzing how privacy expectations should fit in the many other difficult tradeoffs we were making.

Society does, and should, prefer to curtail some liberties in order to save the lives (and, thus, the liberties) of others. Covid-19 has transformed a myriad of 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.

Yet ordinary expectations of data privacy haven’t received the same acid wash of scrutiny: polling suggests that most commentators, including technologists, are still unwilling to think through socially responsible tradeoffs among privacy, human life, other liberties, and economic costs. Instead, a confounding consensus has emerged that even very basic information data should be off the table because of the privacy risks its collection raises even though some of our most fundamental rights have been suspended for weeks and in spite of the fact that many of us willingly share that same information with consumer apps that don’t meet those same standards

Making a Test & Trace system efficacious does not have to mean giving up on privacy, broadly conceived. It only requires considering privacy in the broader context of the dire public health emergency we’re facing and in light of the other substantial compromises we’ve made to address it. Most of the privacy threats raised about digital contact tracing could be guarded against just as well (better, in fact) by strong and verifiable restrictions on how every person’s data is accessed, used, and deleted. In other words, we can protect privacy *without* obstructing a critical tool to manage the public health crisis by using mechanisms other than user choice.