Privacy and Digital Contact Tracing

By Brian Ray (Cleveland State University) and Jane Bambauer (University of Arizona)*

Privacy and Digital Contact Tracing

By Brian Ray (Cleveland State University) and Jane Bambauer (University of Arizona)

Imagine if a major health system developed an app for detecting new cases of COVID-19 more than a week before a person has symptoms or has a viral load large enough to be detected using PCR tests. Users of the app would fill out a baseline questionnaire with their age, BMI, gender, race, ethnicity, occupation, and medical history, and a smartwatch would do most of the work after that. An algorithm would use a broad range of information that many wearable devices like smart watches and Fitbits routinely collect, including heart rate, step counts, sleep patterns and others, to identify that someone likely has contracted COVID-19 up to nine days before they show any symptoms.[1] A more aggressive use of smart devices could even monitor the sound of a cough to detect a COVID infection.[2] Add a daily questionnaire, a button to report the results of any COVID-19 tests, and an automatic contact tracing function and the app would be a huge boon to the management of the epidemic.[3]

These apps leverage the technologies many people routinely use, and the information they already regularly share with private companies for navigation and ad revenues. Surely, we would want to use them to save lives and mitigate the devastating economic effects of the pandemic. Indeed, press accounts of the real apps featuring these powerful tools were positive, highlighting their powerful potential to control the spread of COVID-19.[4]

While an app integrating these functions would collect sensitive personal information, privacy concerns could be managed with relatively routine protections like requiring informed consent, limiting use, and applying the kinds of controls already used to protect sensitive geolocation and health information.

---

*This post is based on our article, *COVID-19 Apps Are Terrible: They Didn't Have to Be*, Lawfare Digital Contract Paper Series (Dec. 2021). Brian Ray would like to acknowledge the Charles Koch Foundation and the Cleveland State University COVID-19 Research Fund for their generous support.

[1] *See* Tejaswini Mishra, *et al*., *Pre-symptomatic detection of COVID-19 from smartwatch data*, 4 Nature Biomedical Engineering 1208 (Nov. 18, 2020), available at https://www.nature.com/articles/s41551-020-00640-6#Abs1.

[2] Jennifer Chu, *Artificial intelligence model detects asymptomatic Covid-19 infections through cellphone-recorded coughs*, MIT News, Oct. 29, 2020, available at https://news.mit.edu/2020/covid-19-cough-cellphone-detection-1029#:~:text=The%20model%20identified%2098.5%20percent,re%20asymptomatic%2C%E2%80%9D%20Subirana%20says.

[3] Robert P. Hirten, *et al., Physiological Data from a Wearable Device Identifies SARS-CoV-2 Infection and Symptoms and Predicts COVID-19 Diagnosis: Observational Study*, J. Med. Internet Res. (2021), available at https://pubmed.ncbi.nlm.nih.gov/33529156/

[4] *See*, *e.g.*, Megan Cerullo, "Smartwatches can help detect COVID-19 days before symptoms appear," CBS News, Jan. 15, 2021; Chance Miller, "New studies show how Apple Watch can help detect COVID-19 prior to symptoms and testing," 9to5Mac, Jan. 16, 2021; Darrell Etherington, "Mount Sinai study finds Apple Watch can predict COVID-19 diagnosis up to a week before testing," Tech Crunch, Feb. 9, 2021

Identifiable information could be destroyed after a short period so that only de-identified and aggregated data is kept for later analysis.

In light of the tremendous potential—the possibility of saving thousands of lives[5]—it would seem unreasonable to declare that the privacy risks should stop us from piloting it. We should at least beta test these tools with large enough numbers of people to ensure they work well enough (and are accountable and privacy-protecting enough, too).

Yet that's precisely what happened with proposals early in the COVID-19 pandemic to repurpose a limited range of location information that people already routinely collect and share with private companies and use it for digital contact tracing. The possibility that such apps could collect location information was dismissed by many decision-makers as too invasive and risky in spite of the fact that these apps could have offered stronger privacy protections than the myriad consumer apps that routinely collect geolocation data.[6] Google and Apple exerted their nearly complete control over the global smartphone market to force governments across the world to abide by this hasty consensus that digital contact tracing apps should be prohibited from collecting location or any information other than anonymized Bluetooth identifiers that could roughly estimate a chance of exposure.

The commentary on digital contact tracing and other tools has shown a puzzling resistance to thinking through how these apps could allow public health officials to collect information responsibly and to aid their efforts to combat the virus while still respecting privacy norms in the public-health context. Instead, a confused coalition has ensured that automatic location tracking data cannot be used for any COVID-related purpose even though public health authorities routinely collect and responsibly use that same information to combat the spread of infectious disease through manual contact tracing and other processes.[7] The consensus that formed made privacy-related tradeoffs impossible, even in the public health context (where tradeoffs have always been necessary), and also stymied the creative approaches

[5] David O. Argente *et al., The Cost of Privacy: Welfare Effects of the Disclosure of COVID-19 Cases,* NBER WORKING PAPER NO. 27220, https://www.nber.org/papers/w27220.
[6] https://www.digitaltrends.com/news/apps-are-tracking-your-location-constantly-and-its-legal/
[7] *See, e.g.*, Dali Kafaar *et al*., "Joint Statement on Contact Tracing: Date 19th April 2020," April 19, 2020, https://giuper.github.io/JointStatement.pdf ("Bluetooth-based solutions for automated contact tracing are strongly preferred [over GPS location] when available."); World Health Organization*, Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance* (May 28, 2020) at 3 ("data collection should not require the identity or location data of a user, or a time stamp of a proximity event"); 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, at 7 ("contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used"), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; Paige Boshell, "The Power of Place: Geolocation Tracking and Privacy," American Bar Ass'n, available at https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/ (describing how private companies collect consumer location data).

that were emerging to responsibly use location and other automatically generated data to reduce the risk of COVID transmission while still protecting privacy.

The result is that the digital contact tracing apps in operation today protect privacy at the expense of efficacy and equity. They are underpowered by design, undersubscribed and ironically untrusted in spite (or perhaps because) of the extraordinary measures these tech giants have taken to protect privacy.[8] As of early 2021, fewer than half of U.S. states even have proposed using a contact tracing or exposure notification app.[9] Even in those, download rates are low and usage rates even lower.[10] These miserable statistics seem to prove correct early critics who argued that proposals to use digital contact tracing to help combat the pandemic were, as one prominent technologist put it, "just plain dumb."[11]

But these statistics are based solely on experience with the specific system that Google and Apple developed and that by design and policy prevents health authorities from using these apps to collect the same kinds of information they already use to understand and prevent the spread of communicable disease. These same limits effectively shut down alternative models that were emerging and that proposed to responsibly collect other information that could have made these apps more effective and accessible and that is critical to help understanding whether these apps work as well as how this disease and the apps themselves affect the most vulnerable communities. Use cases like COVID tracking in South Korea, or like real-time detection of food-borne illnesses here in the U.S.[12], suggested that data from our phones could have and should have been a tool in our arsenal as we combatted waves of coronavirus over the last year.

In January, coronavirus-related deaths peaked at one every twenty-eight seconds in the U.S. COVID-19 alone reduced overall life expectancy of Americans in 2020 by more than one year—the largest single-year decline in the past 40 years.[13] That drop is far worse for communities hit hardest by this disease: falling by over two years for Black Americans and over three years for Latin Americans.[14]

---

[8] *See* Engin Akyurt, *Why people don't trust contact tracing apps and what to do about it*, MIT Tech. Rev., Nov. 12, 2020, at https://www.technologyreview.com/2020/11/12/1012033/why-people-dont-trust-contact-tracing-apps-and-what-to-do-about-it/. https://time.com/5905772/covid-19-contact-tracing-apps/.
[9] *See* Zac Hall, "Which U.S. states are using Apple's Exposure Notification API for COVID-19 contact tracing?," 9to5Mac, Jan. 16, 2021, available at https://9to5mac.com/2021/01/16/covid-19-exposure-notification-api-states/.
[10] *See* Akyurt, *supra* n. 8 (download rates)
[11] Bruce Schneier, "Me on COVID-19 Contact Tracing Apps," Schneier on Security, May 1, 2020, available at https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html. *See also* Ashkan Soltani, et al., "Contact-tracing apps are not a solution to the COVID-19 crisis," Brookings Tech Stream, Apr. 27, 2020, available at https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.
[12] Adam Sadlek, et al., *Machine-learned epidemiology: real-time detection of foodborne illness at scale*, 1 npj Digital Medicine 36 (2018), available at https://www.nature.com/articles/s41746-018-0045-1
[13] *See* Rob Stein, "Pandemic Shortens U.S. Life Expectancy, Study Concludes," NPR, Jan. 15, 2021, available at https://www.npr.org/sections/coronavirus-live-updates/2021/01/15/957209935/pandemic-shortens-u-s-life-expectancy-study-concludes.
[14] *Id.*

Epidemiologists tell us that access to real-time information about who is contracting this deadly disease and where they live, even if it's not granular enough to definitively identify exposure, still can save lives. Would a better digital contact tracing app that included the option for users to collect and share that information with health authorities have made a difference? We can't answer that question definitively. But back in May 2020, when Google and Apple and many others decided the answer must be no, they couldn't have been too well-informed, either.[15]

It's just plain dumb that we never gave them a chance.

Brian Ray
Cleveland-Marshall College of Law
Cleveland State University
b.e.ray@csuohio.edu

Jane Bambauer
James E. Rogers College of Law
University of Arizona
janebambauer@arizona.edu

[15] *See* Jeffrey Khan, *et al.,* Digital Contact Tracing for Pandemic Response Ethics and Governance Guidance, Johns Hopkins University Press (2020) (urging "an approach that recognizes that there are complicated issues to resolve for governments, institutions, and businesses and that introduction of [digital contact tracing technologies] must include public engagement and ongoing assessments to improve both performance and adoption.").