

VIEWPOINT

COVID-19: BEYOND TOMORROW

Digital Smartphone Tracking for COVID-19
Public Health and Civil Liberties in Tension

I. Glenn Cohen, JD
Petrie-Flom Center for
Health Law Policy,
Biotechnology, and
Bioethics, Harvard Law
School, Cambridge,
Massachusetts.

Lawrence O. Gostin, JD
O'Neill Institute for
National and Global
Health Law,
Georgetown University
Law Center,
Washington, DC.

Daniel J. Weitzner, JD
MIT Computer Science
and Artificial
Intelligence Lab,
Cambridge,
Massachusetts.



[Related article](#)



[Supplemental
content](#)

Corresponding

Author: Lawrence O.
Gostin, JD,
Georgetown University
Law Center, 600
New Jersey Ave NW,
McDonough 568,
Washington, DC 20001
([gostin@law.
georgetown.edu](mailto:gostin@law.georgetown.edu)).

Contact investigations have been a vital public health strategy, most recently in controlling tuberculosis and sexually transmitted infections including HIV. Yet, the sheer scale of severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) infections poses major challenges to contact investigations. Strategies in China, Singapore, South Korea, and Taiwan have supplemented traditional manual approaches with digital surveillance through smartphone applications.

The US has not used digital surveillance as a tool, but Google, Apple, the Massachusetts Institute of Technology (MIT), as well as 2 pan-European consortia and a variety of independent efforts are developing Bluetooth smartphone technology to enable rapid notification of users that they have had a close exposure to individuals diagnosed with medically verified coronavirus disease 2019 (COVID-19). How does digital tracking differ from manual tracing? Although digital surveillance has the distinct advantages of scale and speed, does it confer sufficient public health benefit to justify adoption given privacy concerns? How do the design choices of digital contact tracing systems affect public health and privacy?

Comparing Manual and Digital Strategies

Most thoughtful uses of smartphone technologies augment, but do not replace, manual tracing. The most successful strategies begin by massively scaling up manual tracing, as Maryland, Massachusetts, and New York have recently done.¹ Automated systems are designed to add information more rapidly and are scalable to large populations. Traditional tracing begins with reporting to the health department, which then assesses risk, asks diagnosed patients for their known contacts, and notifies contacts of potential exposure, all by telephone call or in person.² Although patients are not usually obligated to disclose their contacts, and health officials do not inform contacts of the patient's name, in some instances those informed can infer who the index patient is.

By contrast, digital tracing rapidly notifies users if they have been in close proximity with a person medically diagnosed with COVID-19. By design, these systems will have layers of privacy protection. Digital tracing will detect proximity, not geographic location, avoiding centralized databases of where smartphone users have traveled. Moreover, downloading and using the smartphone application is voluntary. As a result of recent collaborative efforts by Apple and Google, individuals with iOS or Android smartphones would have the option to turn on tracing similar to the user option to turn on or off location services. The technique for determining proximity relies on anonymous signals (called

"chirps") sent back and forth between phones. Chirps contain no identifying information, safeguarding user privacy. An individual's COVID-19 diagnosis is not revealed except to the public health authorities.³

Digital systems could empower users if public health agencies have oversight of the systems. Apple and Google plans to authorize use of their applications only if health authorities approve. Health officials would define medically significant exposure (distance and time), health messages to identified contacts regarding self-isolation, symptom checks, and notification of medical and public health personnel. The public would have to be assured and trust that Apple, Google, and public health personnel would never use the data for any other purpose.

User Controlled vs Centralized Approaches

Two contrasting approaches to digital contact tracing have emerged: a more centralized approach favored by governments in China, South Korea, Taiwan, and elsewhere and a decentralized, user-centric approach supported by the joint Apple-Google system and favored by some, but not all, European countries (eTable in the [Supplement](#)). China, for example, combined government surveillance of the location histories for individuals to create infection risk scoring systems, and now requires its citizens to score "green" to enter public facilities, workplaces, or travel. South Korea's digital surveillance uses law enforcement and fines to sanction individuals who violate quarantine or social distancing orders. Taiwan added smartphone location tracking to detect and sanction quarantine violations. Israel initially used national security legal authority for the Ministry of Health to implement digital tracking, but recently the Israeli High Court of Justice found that the surveillance, conducted as it was under an executive order and absent legislative approval, lacked adequate legal basis to continue.⁴⁻⁶ Importantly, every successful implementation of digital systems relied also on well-resourced and rapidly deployed manual contact tracing.⁷

A divide has emerged in Europe over the design of automated tracing systems. Countries agree that digital systems are needed to automatically identify contacts of infected individuals but disagree about how much personal information health authorities should receive without individual consent. Some governments (eg, France, Italy, and the UK) favor more centralization in which public health departments immediately receive personal information about identified contacts. Other governments (eg, Austria, Estonia, Germany, and Switzerland) favor decentralization following a design from a group of European academics called DT-3P in which contacts receive notification of their proximity to infected people, but health authorities are notified only

if the individual chooses to do so. The Apple, Google, and MIT designs are aligned with this decentralized approach. In the US, the federal government has yet to announce a nationwide policy.

Optimal Design: Balancing Health and Privacy

Despite scientific uncertainty, digital systems could significantly contribute to curtailing the spread of SARS-CoV-2 infection if adopted widely and integrated into comprehensive public health strategies. Ultimately, there may be trade-offs between public health efficacy and privacy-enhancing features.

Digital tracing should augment traditional public health strategies but cannot replace them. Primary public health strategies include widescale population testing, manual tracing, isolation, and quarantine. Social distancing also remains important for mitigating spread and maintaining health system capacities. As important as opening the economy may be, overreliance on digital tracking alone will result in a resurgence of cases and increased stress on the hospital system.

Digital systems cannot effectively augment traditional methods without widespread uptake. A recent simulation suggests the COVID-19 pandemic can be suppressed with 80% of all smartphone users utilizing the application, or 56% of the overall population.⁸ A voluntary system without effective incentives is unlikely to achieve sufficient uptake, although partial benefits could accrue at lower levels of uptake. Early results from Singapore's voluntary system have shown only 20% of the population had installed the application as of April 21, 2020.⁹ The US public is unlikely to accept mandates to implement digital tracing, even in a health emergency. Maintaining public trust remains a vital component of COVID-19 pandemic control.

Because a critical mass of users will not be in the network at the requisite time, and some individuals will not register a COVID-19 diagnosis, digital systems alone cannot ensure safety. Public health officials must educate the public about the deficiencies of voluntary tracking systems. Otherwise, the public could gain a false sense of

security, which could encourage increased risk-taking behaviors. The average user, not knowing the size of the network or sharing rates, will find it difficult to interpret feedback from the digital application.

Although digital tracking has been designed as a public health tool, it will be important to avoid secondary uses, such as in the workplace, law enforcement, or immigration. Employers may ask for results from smartphone applications as a condition of return to work. Hospitals might consider results in prioritizing testing and treatment. Neither is warranted given the current state of the technology. Ensuring robust legal protection against privacy invasions and unauthorized use will enhance social acceptance of digital systems.

Once an application is in the public sphere, it could remain a long-term feature in the smartphone environment. To avoid long-term uses, so-called function creep, especially for nonpublic health purposes, federal or state authorization for digital applications could be tied to the duration of COVID-19 emergency declarations with an automatic sunset in place. Applications could also be designed to automatically uninstall after a fixed period and the personal data could be automatically erased.

Trade-off Between Civil Liberties and Public Health

Although it is conceivable to envisage public health and civil liberties as synergistic, they often are in tension. To improve uptake, governments could mandate or incentivize use of these technologies and permit data uses by employers and businesses. State health departments could also seek access to digital data for wider surveillance purposes. Given the current evidence base behind these digital methods, it would be premature to mandate their use, thus the trade-off between privacy and autonomy for uncertain public health benefits. Incentives seem more plausible. Widespread deployment would only be warranted if pilot projects and modeling offer sufficient scientific evidence to assess public health efficacy against privacy and other costs.

ARTICLE INFORMATION

Published Online: May 27, 2020.
doi:10.1001/jama.2020.8570

Conflict of Interests Disclosures: Mr Cohen reported serving as a bioethics consultant for Otsuka on its Abilify MyCite product. Mr Gostin reported being the director of the World Health Organization Collaborating Center on National and Global Health Law. Mr Weitzner reported being co-principal investigator on the MIT PACT project (<https://pact.mit.edu/>), which is one of the technologies discussed in this article.

Funding/Support: Mr Cohen was supported by the Collaborative Research Program for Biomedical Innovation Law, a scientifically independent collaborative research program, which is supported by grant NNF17SA0027784 from the Novo Nordisk Foundation. Mr Weitzner's research group, the MIT Internet Policy Research Initiative, was supported by a grant from the MIT-IBM Watson AI Lab for COVID-19 efforts.

Role of the Funders/Sponsors: The funders/sponsors had no role in the preparation, review, or approval of the manuscript or decision to submit the manuscript for publication.

REFERENCES

1. Faulders K, Pecorin A, Kim SR, Rubin O. States race to start coronavirus testing, a monumental task ahead. Accessed April 22, 2020. <https://abcnews.go.com/US/states-race-start-coronavirus-contact-tracing-monumental-task/story?id=70285156>
2. Contact tracing of cases of AIDS, HIV related illness or HIV infection. *NY Pub Health Law* §2133.
3. Bond S. Getting back to normal: big tech's solution depends on public trust. Accessed April 10, 2020. <https://www.npr.org/2020/04/14/834460127/apple-google-team-up-to-develop-cellphone-data-contact-tracing>
4. Park S, Choi GJ, Ko H. Information technology-based tracing strategy in response to COVID-19 in South Korea—privacy controversies. *JAMA*. Published online April 23, 2020. doi:10.1001/jama.2020.6602
5. Klimburg A, Faesen L, Verhage P. Pandemic mitigation in the digital age: digital epidemiological measures to combat the coronavirus pandemic. Accessed April 25, 2020. <https://hcsc.nl/report/pandemic-mitigation-digital-age>
6. Haaretz website. Israel's Top Court: No Shin Bet Tracking of Coronavirus Patients Without Knesset Oversight. Accessed May 25, 2020. <https://www.haaretz.com/israel-news/.premium-israel-s-top-court-no-shin-bet-tracking-of-coronavirus-patients-without-knesset-ove-1.8690253>
7. Watson C, Cicero A, Blumenstock J, Fraser M. A national plan to enable comprehensive COVID-19 case finding and contact tracing in the US. Accessed April 25, 2020. https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf
8. Ferretti L, Wymant C, Kendall M, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*. 2020;368(6491):eabb6936. doi:10.1126/science.abb6936
9. Fernandez E. Privacy and contact tracing apps—Google and Apple debate with world governments. Accessed April 24, 2020. <https://www.forbes.com/sites/fernandezelizabeth/2020/04/24/privacy-and-contact-tracing-apps-google-and-apple-debate-with-world-governments/#306208f94518>