Surveillance, Privacy, and App Tracking

Jennifer D. Oliva, JD, MBA, Seton Hall University School of Law

SUMMARY. Over the last several months, global innovators have developed a heterogenous array of "smart" technology protocols and applications aimed at tracking, tracing, and containing the spread of the novel coronavirus, SARS-CoV-2, which causes the disease COVID-19. The United States, which has left it to the states to acquire or build their own automated track and trace platforms, currently lags behind other countries. However, technology companies Apple and Google have announced co-production of a digital tracing platform for their phones. As this Chapter details, the United States lacks a comprehensive federal health data privacy law that protects the privacy of sensitive information collected and stored by digital contact tracking applications. The Chapter also explains how digital COVID-19 surveillance applications work, assesses their effectiveness from a public health perspective, and enumerates the legal and ethical issues they implicate. It concludes with proposals aimed at maximizing the public health benefits of COVID-19 surveillance technology while minimizing its inherent and conceivable threats to privacy, civil liberties, and vulnerable populations.

Introduction

Traditional contact or "case" tracing is a long-standing pillar of public health infectious disease prevention and mitigation dating back at least 500 years to medieval European bubonic plague outbreaks (Cohn & O'Brien, 2020). It is a multi-step process involving the deployment of an army of public health workers tasked with (1) identifying infected individuals; (2) interviewing infected individuals to identify others with whom they have had contact; and (3) testing and isolating those people to stem the tide of disease.

Government public health surveillance can detect and mitigate the spread of contagion, encourage health-enhancing behavioral, social, and environmental interventions, influence disease-mitigation law and policy, promote economic recovery, and protect high-risk populations (Gostin & Wiley, 2016). The system and its social benefits, however, are not without their detractors. Traditional contract tracing is expensive and resource intensive, and has been characterized as "slow," "passive," and "riddled with holes" (Shah, 2016).

Such holes are frequently exacerbated by traditional contact tracing's necessary reliance on (1) accurate, widespread, and timely testing and (2) public trust in government sufficient to encourage meaningful screening, testing and reporting. The United States, which was criticized for its failure to widely screen its population early in its COVID-19 response, still lacks a unified national testing strategy. The states have stepped into the void and dramatically increased testing to track viral transmission and facilitate contact tracing as they have moved to reopen (Nuzzo, 2020).

The jury, however, is still out regarding the accuracy of screening tests (Modern Healthcare, 2020). Additional complicating factors include the notoriously long waits that have attended to tests results and the lack of any standardized national criteria as to what constitutes a COVID-19 "case" in the first instance. The threshold identification of a "case" subject to track and trace, therefore, is likely to vary across states as well as within states that have delegated such determinations to local government entities. Equally problematic, there is considerable public distrust in contact tracing in the United States due to political polarization and rampant social media disinformation (Appleby, 2020).

Even assuming the existence of a standardized definition of a "case," fast, widespread, and accurate COVID-19 testing, and sufficient public trust to facilitate contact tracing, those who are asymptomatic and have not been tested have nothing to report. Individuals with mild to moderate symptoms also are disincentivized to subject themselves to screening, testing, and tracing because infectious disease surveillance can implicate the right to critical benefits, including access to employment, housing, and insurance (Gostin & Wiley, 2016). Because of the voluminous amount and sensitive nature of the data public health surveillance systems collect, traditional track and trace also raises ethical concerns that can disproportionately impact vulnerable groups, including low income and rural communities and individuals with legal status issues, stigmatizing co-morbid conditions or disabilities, and/or above-average contact with the criminal justice system.

These traditional contract tracing shortcomings have provoked American policymakers to look to digital containment tools,

including high-tech surveillance applications, to contain the spread of COVID-19. In April 2020, technology behemoths Google and Apple announced their co-production of application programming interfaces (APIs) for mobile Bluetooth technology surveillance to mitigate COVID-19 transmission. The voluminous proliferation of these digital surveillance applications precipitated the Massachusetts Institute of Technology's creation of a COVID Tracing Tracker to "capture every . . . automated contact tracing effort around the world," (O'Neill et al., 2020). As things currently stand, however, only four state public health authorities have reported that they intend to utilize Google/Apple exposure notification APIs (Hall, 2020).

Digital application surveillance is potentially cheaper and faster—and arguably more comprehensive and precise—than traditional track and trace because automated data collection does not rely on the limitations of human memory or reporting. Unfortunately, and as explained below, digital applications raise novel accuracy problems attributable to their underlying technology. They also routinely exclude high-risk individuals who lack access to technology and implicate heightened privacy and civil liberties concerns relative to traditional surveillance. The significant privacy and civil liberties risks raised by digital contact tracing technology are driven by a pair of intersecting factors. First, unlike traditional surveillance, which is conducted by health authorities for the exclusive purpose of containing infectious disease, most digital track and trace applications are the products of private technology companies whose business models have long been dependent on monetizing consumer data. Second, the constitutional and decades-old statutory health data privacy protections that extend to traditional health care actors in the United States generally do not apply to information collected and stored by private entities. The country's inadequate and patchwork-like health data protections laws are summarized in the following Section.

U.S. Health Data Privacy Law

Federal Constitutional Rights

While the U.S. Constitution does not expressly recognize a right to informational privacy, the Supreme Court identified a qualified right to health data privacy in *Whalen v. Roe*. At issue in *Whalen* was a New York statute that required physicians to report patient drug-prescribing information to the state department of health. Patients and physicians challenged the law on the grounds that it violated their Fourteenth Amendment rights to "nondisclosure of private information" (*Whalen v. Roe*, 1977). The Court rejected that argument but, in so doing, recognized that (1) individuals have Fourteenth Amendment privacy interests in their health data and (2) the compulsory disclosure of such data to a state public health agency satisfies the Fourteenth Amendment so long as the health agency safeguards the information it collects from public disclosure (Oliva, 2020).

The Supreme Court has also recognized that individuals have a reasonable expectation of privacy in their health data under the Fourth Amendment to the U.S. Constitution. In *Ferguson v. City of Charleston*, for example, the Court held that a state hospital violated patients' Fourth Amendment privacy rights by sharing patients' diagnostic test records "with nonmedical personnel without [their] consent" (*Ferguson v. City of Charleston*, 2001). More recently, the Court held in *Carpenter v. United States* that individuals have a Fourth Amendment privacy interest in their cell site location information (CSLI) even when those records reveal public movements (*Carpenter v. United States*, 2018). These Fourteenth and Fourth Amendment privacy protections, however, apply only to government actors and not to the actions of private entities or employers. In addition, there are special needs and immigration-related exceptions to the Fourth Amendment warrant requirement that lessen privacy protections for individuals at or about the U.S. border (*United States v. Flores-Montano*, 2004).

HIPAA Privacy Rule

Unlike the European Union, which enacted the General Data Protection Regulation (GDPR) effective May 25, 2018, the United States lacks a comprehensive and effective data privacy law. The federal statute that is popularly synonymous with health information privacy is the Health Insurance Portability and Accountability Act. HIPAA however, only applies to a narrow sub-set of individually-identifying health data, which the statutory scheme refers to as "protected health information" (PHI), and a limited set of actors integral to the traditional health care payment system: health care providers, plans, clearinghouses, and their "business associates." HIPAA, which was enacted in advance of the advent of mobile devices and big data analytics, fails to extend to myriad private entities that collect, store, and sell health data, including digital health care application information (Terry, 2020).

The HIPAA Privacy Rule is riddled with numerous public purpose exceptions. Those exceptions allow covered entities to use and disclose PHI for, among other things, health oversight activities, judicial and administrative proceedings, law enforcement purposes, limited research activities, specialized government functions, and the aversion of serious threats to health or safety. Individuals who are justice involved and/or have legal status issues, therefore, are particularly vulnerable to nonconsensual HIPAA disclosures. HIPAA also fails to include a private right of action.

State Health Data Protection Laws

Adding to the complex patchwork of federal laws, several American states have recognized a state constitutional right to health data privacy, and most have developed statutory frameworks for data protection (Glenn, 2000; Terry, 2009). California recently adopted the most comprehensive state-level data protection regime in the United States by enacting the California Consumer Privacy Act (CCPA). While that law expressly exempts from its purview HIPAA-covered entities and health data governed by the state Confidentiality of Medical Information Act, it does apply to private digital application developers who conduct substantial business in California. It creates, among other things, the right to correct data, delete data, and privately enforce statutory privacy violations. The CCPA does not, however, extend to consumers any right regarding de-identified information.

The Exposure Notification Privacy Act

Congress has acknowledged that the above-described American privacy protection scheme is inadequate to safeguard individuals from the risks that attend to digital COVID-19 contact tracing applications. On June 1, 2020, two senators introduced the Exposure Notification Privacy Act (ENPA), which aims to "give[ ] Americans control over their data [and] put[ ] public health officials in the driver's seat of exposure notification development." ENPA is the third bill designed to protect health data privacy in the context of COVID-19 that Congress has introduced since April 30, 2020. The legislation requires automated exposure notification application operators to (1) collaborate with public health authorities, (2) obtain consent from enrolled users as well as a "clear and conspicuous" means to withdrawal such consent, (3) refrain from any data collection beyond that which is minimally necessary to implement the application, (4) abjure the use of such data for commercial purposes, (5) delete the data on regular intervals, and (6) permit users to request data deletion. The statute does not provide individuals with a private right of action to enforce its privacy protections.

COVID-19 Digital Surveillance & Tracking Technology

The two prevalent forms of automated contact tracing technology that have been designed and proposed for use to mitigate the spread of COVID-19 are location tracking applications and proximity tracking applications. Location tracking applications use global positioning system (GPS) and CSLI data generated by smartphones to track users' physical movements. Location tracking applications are generally disfavored on both effectiveness and privacy grounds because, while GPS and CSLI-generated data are accurate enough to reveal troves of sensitive user information, it reliably fails to identify whether two individuals have engaged in close enough contact (six feet) to transmit COVID-19 (EFF, 2020). In addition, the Supreme Court has extended Fourth Amendment privacy protection to CSLI and GSP at least insofar as that data is collected and used for law enforcement purposes over an extended period of time. Whether the administrative search or special needs doctrines would exempt such data collected and used exclusively for public health surveillance purposes from Fourth Amendment purview is a more difficult and unsettled question.

Proximity tracking applications have emerged as the preferred option among developers and public health authorities. These applications use the strength of Bluetooth signals emitted by users' smartphones to approximate the distance between two devices. Many proximity tracking designs, including the API protocols developed by Apple and Google, create a unique smartphone identifier and then routinely rotate those identifiers to enhance user privacy. Once a proximity application estimates that users are less than six feet apart for a sufficient period of time, it logs the interaction and exchanges the users' unique identifiers between their phones. Proximity tracking need not involve the collection of users' actual physical locations. The exposure notification system instead relies entirely on the length of time and proximity of user contacts generated by their smartphones' Bluetooth signals.

It is at this stage of the data collection process that proximity tracking applications tend to vary. Some applications, such as Singapore's "TraceTogether" technology are based on "top-down" or "centralized" notification. These systems trust a central authority, such as a public health agency, with users' contact (phone numbers, email addresses, etc.) and testing information. Once a TraceTogether user tests positive for COVID-19, that information is shared with the Singapore Ministry of Health, which, in turn, contacts each of the infected users' logged contacts by phone or email.

Alternative approaches tend to be more decentralized and shelter more information from authorities. For example, in lieu of storing actual user contact information with a central authority, certain proximity tracking applications allow infected users to upload their own de-identified contact logs to a centralized database. The central authority then "notifies" or pings all at-risk users using each user's unique identifier. Apple and Google's joint approach goes even further. It creates a public database that broadcasts the unique identifiers of infected users to the smartphone applications of those with whom infected users come in close proximity.

The decentralized proximity tracking applications alleviate some—but not all—of the privacy concerns raised by governmental collection and storage of health data. Re-identification techniques are so widespread and effective, however, that the provision of even minimum personal data to a central authority via unsophisticated decentralized systems risks user identification. These concerns can and should be mitigated with robust encryption security safeguards.

Other pertinent issues that could undermine the efficacy of these systems pose more difficult challenges. First, and as alluded to above, proximity tracking applications are ineffective without fast, accurate, and widely available COVID-19 testing, which the United States does not currently have in place. Second, digital tracing applications cannot succeed without widespread adoption premised on public trust of the technology in the hands of governmental actors. "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," and, as several renowned health law scholars recently warned, the U.S. "public is unlikely to accept mandates to implement digital tracing, even in a health emergency" (Cohen et al., 2020).

Third, proximity tracking applications risk both over- and under-inclusive exposure notification. They run into over-inclusivity issues because Bluetooth signals cannot meaningfully distinguish between individuals who actually come into prolonged and proximate contact and individuals who are separated by walls or are in different cars in parallel lanes on a road. The applications also cannot detect whether one or both of the users is wearing personal protective equipment (PPE). They are, therefore, likely to produce a high number of alerts for health care and other essential workers who frequently interact with others even when they are adequately protected with PPE.

Because they track the distance between smartphones and not the distance between human users, proximity tracking applications are also likely to generate under-inclusive exposure notifications. Users who fail to keep their smartphones on their persons when interacting with others are likely to be under-notified by the system as well as cause their contacts to be under-notified. In addition,

individuals whose interactions would qualify as a notification "contact" for digital tracing purposes will fall through the net to the extent that they are using different proximity applications.

More problematic, digital surveillance applications systematically exclude groups often at high-risk of COVID-19 exposure but least likely to have a smartphone and/or adequate data plan, including elderly people, low-income individuals, people with legal status issues, and individuals who live in rural communities. Digital track and trace systems, therefore, must offer these vulnerable groups free devices and data plans. Certain individuals are likely to opt out of even cost-free electronic surveillance. Low-wage and immigrant workers, for example, are at high-risk of non-participation because it is often impracticable for them to shelter in place for a two-week period and retain their employment and housing. Those with legal status issues or who are involved with the criminal legal/justice system are further incentivized to avoid surveillance out of fear of immigration authority and law enforcement reprisal. Finally, as noted above, a substantial segment of the American public will opt-out of digital track and trace because of their distrust of government monitoring.

Conclusion

The high value of protected health information, its extraordinary sensitivity, the United States' lack of comprehensive health data protection laws and regulations, and significant efficacy and privacy issues raise serious concerns about digital contact tracing applications. Drawing from thoughtful discussions advanced by the Electronic Frontier Foundation, American Civil Liberties Union, European Data Protection Board, and International Association of Privacy Professionals, this Chapter concludes with a series of recommendations aimed at safeguarding against the risks posed to individuals by digital infectious disease surveillance while maximizing its public health benefits.

Recommendations for Action

Federal government:

- To facilitate appropriate use of technology in pandemic control, Congress should enact a statute that safeguards individuals from the risks that attend to digital COVID-19 contact tracing applications. Legislation should:
  - Ensure user privacy;
  - Assure informed, voluntary participation;
  - Respect user autonomy;
  - Prohibit discrimination and the dissemination of collected information to non-public health authorities;
  - Prescribe the commercial use of collected data, mandate government transparency and accuracy, and guarantee data security;
  - Include a sunset provision; and
  - Extend to users a private right of action.

State governments:

- In the absence of federal action to facilitate appropriate use of technology in pandemic control, states should enact a statute that safeguards individuals from the risks that attend to digital COVID-19 contact tracing applications. Legislation should:
  - Ensure user privacy including,
    - Data minimization;
    - Data deletion and correction;
    - Information security, including compliance with international data security best practices, encryption, conduct penetration tests and audited vulnerability assessments, and data breach notification; and
    - Extending to users a privacy right of action.
  - Assure informed, voluntary participation.
  - Respect user autonomy.
  - Prohibit discrimination and the dissemination of collected information to non-public health authorities.
  - Prescribe the commercial use of collected data, mandate government transparency and accuracy, guarantee data security.
  - Include a sunset provision, and
- To ensure that contract tracing apps and processes do not reflect bias or infringe upon civil liberties and human rights, state governments by legislation or agency rule should ensure that as implemented:
  - Applications neither (1) intentionally nor disparately burden folks on the basis of race, ethnicity, nationality, sex, religion, immigration status, LGBTQA+ status, or disability, nor (2) document information that implicates users' civil liberties or human rights
  - Health authorities should provide no-cost cellular phones and data packages to individuals who wish to participate but do not have the resources to obtain the underlying technology, devices, and data plans
  - Health authorities should incorporate the use of traditional contact tracers with local connections to vulnerable communities rather than solely rely on automated surveillance to ensure the inclusion of individuals who do not have access to smartphone technology and/or otherwise distrust digital surveillance.
- State governments (or, if it enters this space, the federal government) that implement digital contact tracing:
  - Should also implement accurate, fast and widespread COVID-19 testing;
  - Only adopt applications that are accurate enough that they assist rather than undermine traditional contract track and trace efforts;
  - Should respect autonomy/informed consent:
    - Application usage should be voluntary and expressly permit users to opt-in and opt-out.
    - Application terms and conditions/user agreements should be clear and transparent and accessible to individuals with disabilities.
    - Application terms and conditions/user agreements should be translated into the most common languages and health authorities should ensure that translators are available to assist individuals to understand consent forms.
  - Prioritize Anti-Bias, Civil Liberties, and Human Rights Protections
    - Applications should neither (1) intentionally nor disparately burden folks on the basis of

State recommendations, continued

race, ethnicity, nationality, sex, religion, immigration status, LGBTQA+ status, or disability, nor (2) document information that implicates users' civil liberties or human rights

- Health authorities should incorporate the use of traditional contact tracers with local connections to vulnerable communities rather than solely rely on automated surveillance to ensure the inclusion of individuals who do not have access to smartphone technology and/or otherwise distrust digital surveillance. As a recent EFF article explains, "[w]e cannot solve a pandemic by coding the perfect app. Hard societal problems are not solved by magical technology, among other reasons because not everyone will have access to the necessary smartphones and infrastructure to make this work," (Crocker et al., 2020).

About the Author

Jennifer D. Oliva, specializes in health law and policy, FDA law, evidence, complex litigation, and privacy. Professor Oliva earned her JD from Georgetown University Law Center, where she was a Public Interest Law Scholar and Executive Notes & Comments Editor of *The Georgetown Law Journal*. Prior to attending law school, she earned an MBA from the University of Oxford and was selected as a Rhodes and Truman Scholar while a cadet at the United States Military Academy. Her work has been published by or is forthcoming in the *Duke Law Journal*, *Northwestern University Law Review*, *Ohio State Law Journal*, *Washington Law Review*, *North Carolina Law Review*, and online companion to the *University of Chicago Law Review*.

References

Apple (2020). Apple and Google Partner on COVID-19 Contact Tracing Technology. Retrieved July 13, 2020, from https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Appleby, J. (2020). Conspiracy Theories Aside, Here's What Contact Tracers Really Do. Retrieved July 28, 2020, from https://californiahealthline.org/news/conspiracy-theories-aside-heres-what-contact-tracers-really-do/

Blumenthal, D., & Blumenthal, R. (2020). Contact Tracing Must Balance Privacy and Public Health. Retrieved July 13, 2020, from https://www.statnews.com/2020/05/15/contact-tracing-must-balance-privacy-and-public-health/

California Consumer Privacy Act, California Civil Code § § 1798.100-1798.199 (2018).

Carpenter v. United States, 138 S. Ct. 2206 (2018).

Children's Online Privacy Protection Act, 15 U.S.C. § § 6501-6506 (1998).

Cohen I.G., Gostin, L.O., & Weitzner, D.J. (2020). Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension. *Journal of the American Medical Association*, 323(23), 2371-2372. Retrieved July 13, 2020, from https://jamanetwork.com/journals/jama/fullarticle/2766675

Cohn, S., & O'Brien, M. (2020). Contact Tracing: How Physicians Used it 500 Years Ago to Control the Bubonic Plague. Retrieved July 13, 2020, from https://theconversation.com/contact-tracing-how-physicians-used-it-500-years-ago-to-control-the-bubonic-plague-139248

Crocker, A., Opshal, K., & Cyphers, B. (2020). The Challenge of Proximity Apps for COVID-19 Contact Tracing. Retrieved July 28, 2020, from https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

Electronic Frontier Foundation. (2020). Guide to Digital Rights During the Pandemic: An eBook. Retrieved July 13, 2020, from https://www.eff.org/pages/guide-digital-rights-pandemic

Exposure Notification Privacy Act, S.3861, 116th Cong. (2020).

Family Educational Rights and Privacy Act, 10 U.S.C. §1232g (2013).

Ferguson v. City of Charleston, 532 U.S. 67 (2001).

Glenn, C.L. (2000). Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records. *Vanderbilt Law Review*, 53(5), 1605-1635.

Gostin, L.O., & Wiley, L.F. (2016). Public Health Law: Power, Duty, Restraint. Oakland, CA: University of California Press.

Hall, Z. (2020). Which U.S. States are Using Apple's Exposure Notification API for COVID-19 Contact Tracing? Retrieved July 28, 2020, from https://9to5mac.com/2020/07/13/covid-19-exposure-notification-api-states/

Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

Johnson, B. (2020). The US Draft Law on Contract Tracing Apps is a Step Behind Apple and Google. Retrieved July 13, 2020, from https://www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/

Modern Healthcare (2020). Accuracy of COVID-19 Tests Still Largely Unknown. Retrieved July 13, 2020, from https://www.modernhealthcare.com/technology/accuracy-covid-19-tests-still-largely-unknown

Nuzzo, J.B. (2020). No, More Testing Doesn't Explain the Rise of COVID-19 Cases in the U.S. *Washington Post*. Retrieved July 13, 2020, from https://www.washingtonpost.com/outlook/2020/06/22/no-more-testing-doesnt-explain-rise-covid-19-cases-us/

O'Neill, P.H., Ryan-Mosley, T., & Johnson, B. (2020). A Flood of Coronavirus Apps are Tracking Us. Now It's Time to Keep Track of Them. Retrieved July 13, 2020, from https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Oliva, J.D. (2020). Prescription-Drug Policing: The Right to Health-Information Privacy Pre- and Post-Carpenter. *Duke Law Journal*, 69(4), 775-853.

Privacy Act, 5 U.S.C. § 552a (1974).

Shah, S. (2016). Pandemic: Tracking Contagions, from Cholera to Ebola and Beyond. New York, NY: Picador.

Terry, N.P. (2009). What's Wrong with Health Privacy? *Journal of Health and Biomedical Law*, 5(1), 1-32.

Terry, N.P. (2020). Assessing the Thin Regulation of Consumer-Facing Health Technologies. *Journal of Law, Medicine and Ethics*, 48(S1), 94-102.

United States v. Flores-Montano, 541 U.S. 149 (2004).

Whalen v. Roe, 429 U.S. 589 (1977).