Surveillance, Privacy, and App Tracking

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

SUMMARY. As the COVID-19 pandemic swept across the United States, American policymakers expressed optimism that digital contact tracing applications would mitigate the spread of the virus. Despite such hope, digital tracing tools have played virtually no role in reducing the transmission of COVID-19. This Chapter details the challenges faced and posed by digital contact tracing, exposes and criticizes its threats to stigmatized and marginalized populations, summarizes the lessons learned from our failed experiment with digital tracing in the context of COVID-19, and provides recommendations aimed at empowering the country to harness digital surveillance to stymie the spread of contagious disease when the next pandemic arrives.

Introduction
As explained in Volume I, Chapter 5, effective contact tracing demands several prerequisites. Contact tracing cannot succeed without accurate, widespread, and timely testing throughout the community. Unfortunately, the United States abdicated its duty to implement a coordinated national testing plan. The federal government consigned COVID-19 testing and tracing operations to the overwhelmed and often under-resourced states (Salomon & Reingold, 2020). The states, in turn, struggled during the first several months of the pandemic to develop standardized criteria as to what constitutes a COVID-19 “case,” adequately test their constituents, and timely return test results. As various regions of the country witnessed viral surges over the summer and fall of 2020, these testing problems escalated, and over-stretched state public health officials were compelled to either scale back or abandon traditional contact tracing (Woodward, 2020). Questions about the accuracy of the tests that the U.S. Food and Drug Administration (FDA) authorized for use through its national public health emergency powers exacerbated the states’ testing woes.

Contact tracing also requires honest participation from individuals who have been exposed to the disease, which is catalyzed by fear of stigmatization. The sensitive data collected by government officials has stymied efforts to track, trace, and contain the spread of the SARS-CoV-2 virus in the United States. Marginalized groups that have been disparately impacted by the virus and historically targeted by law enforcement and other surveillance agencies are concerned that police and immigration authorities will exploit contact tracing data to their detriment. Political polarization and social media propaganda have further eroded distrust in public health officials. As the 2020 winter holidays approached, the country’s COVID-19 case count exceeded 200,000 a day and the United States witnessed record hospitalizations and deaths. However, a vocal minority of Americans, inclusive of various elected officials, continues to subscribe to the theory that the virus is a hoax and refuses to comply with basic transmission prevention tactics (Enriquez, 2021).

These obstacles to traditional contact tracing motivated policymakers to look to digital contact tracing applications to contain the spread of COVID-19. Digital surveillance tools are enticing because they are faster and less resource intensive than traditional track and trace methods. They nonetheless suffer notable drawbacks. First, digital exposure notification platforms are likely to generate both false negatives and false positives due to the nature and limits of their underlying technology. Second, the collection, storage, and aggregation of sensitive health and location data by digital applications raises novel privacy issues that the American health data privacy legal regime is ill-equipped to manage. Third, digital platforms exclude vulnerable individuals who are at high-risk of COVID-19 exposure but do not have access to the technology and data plans necessary to participate in mobile tracing. Finally, and like traditional contact tracing, digital contact tracing applications cannot effectively reduce viral spread without adequate community testing and public trust in both the government and the private companies that develop the platforms sufficient to motivate their widespread use. These issues that attend to digital contact tracing have colluded to minimize their use and effectiveness in the United States to date. For additional information on surveillance, privacy, and app tracking, please see Chapter 5 in Assessing Legal Responses to COVID-19: Volume I.

Updates
Since the publication of the first volume of this playbook, digital contact tracing has remained a persistent and unwavering failure. Perhaps because we are primed to believe that technology will rescue us, there was significant optimism that Big Tech’s development and release of a decentralized framework for contact tracing applications in April 2020 would be a game changer in the fight against COVID-19. As it turns out, that optimism was tragically misplaced.
A year into the pandemic, “such apps have made slow progress across the country, hampered by sluggish and uncoordinated development, distrust of technology companies, and inadequate advertising budgets and messaging campaigns” (de la Garza, 2020). Recent reports indicate that only 18 states have adopted digital contact tracing applications and, in those states, only one in 14 residents have uploaded and utilized the technology (Mello, Jr., 2020). Connecticut currently stands as the most successful digital application state in the nation, with just a 20% adoption rate (Mello, Jr., 2020). While traditional contact tracing has fared somewhat better than its digital counterparts, it also has faced considerable resistance. More than half of Americans who have become infected with COVID-19 have refused to cooperate with contact tracers (Lewis, 2020).

At the pandemic’s inception, there also was hope that the United States would update its fragmented and inadequate health data privacy regime to bolster user privacy and, thereby, instill public trust in digital tracing applications. At least three bills that sought to regulate the use of contact tracking data, including the bipartisan Exposure Notification Privacy Act, were introduced in the Senate. None of that proposed legislation, however, gained traction in Congress. To be fair, the enactment of a federal privacy law that protects the sensitive health data collected by digital applications would not solve all the problems that have stymied the success of digital contact tracing. Federal action on this front, however, is long overdue. Moreover, protection of such individual health and location data is likely to benefit members of marginalized communities who are most likely to be subject to punitive state action, have suffered disproportionately during the pandemic due to systemic disparities in the health care delivery system, and are the subject of the next section of this Chapter.

Equity

The data overwhelmingly demonstrate that COVID-19 has disparately impacted various groups that have experienced historical stigma, discrimination, and abuse, including racial and ethnic minorities, individuals with disfavored health care conditions and criminal statues, and older Americans. Pandemic-related inequitable health outcomes are attributable to, among other things, structural racism, ableism, ageism, and long-standing economic inequality.

“These systems affect health through a variety of pathways, including social deprivation from reduced access to employment, housing, and education; increased environmental exposures and targeted marketing of unhealthy substances; inadequate access to health care; physical injury and psychological trauma resulting from state-sanctioned violence such as police brutality and chronic exposure to discrimination; and diminished participation in healthy behaviors or increased participation in unhealthy behaviors as coping mechanisms.” (Egede, 2020).

Digital contact tracing poses specific risks to these same populations. Communicable disease epidemics generally trigger widespread fear and the spread of insidious misinformation that unfairly blames marginalized groups for spread of the contagion. As early as the mid-1300s, white Europeans blamed Jewish people for transmission of the bubonic plague throughout the continent (McNeil, Jr., 2009). Americans scapegoated Haitian immigrants and sexual minorities as responsible for HIV transmission in the 1980s (Cohen, 2007). The same fate attended to Mexican Americans during the 2009 swine flu outbreak, West Africans during the 2014 Ebola epidemic, and, of course, Chinese Americans during the COVID-19 pandemic (Lee, 2020). These attacks on marginalized groups during public health emergencies incentivizes them to avoid data collection due to fear of law enforcement dragnets and other punitive measures.

American policymakers have made little effort to quell such targeting of stigmatized groups during the pandemic. In the face of widespread outbreaks of COVID-19 in U.S. meatpacking plants, which rely heavily on immigrant and racial minority labor, government officials placed the blame for viral transmission not at the feet of the employers who maintain non-hygienic and cramped work conditions, but on the immigrant workers who must endure those unsafe work environments (Stella, 2020). Meatpacking plants have long been subject to immigration sweeps by federal authorities. It is irrational to expect groups at heightened risk of criminalization, detention, and deportation to use digital tracking tools. That result, however, is counterproductive because an environment that motivates disease surveillance avoidance exacerbates the potential for poor public health outcomes for these workers and their families and heightens the risk of undetected viral spread throughout the community. In fact, Singapore experienced a surge of COVID-19 cases in the spring of 2020 linked to migrant workers living in cramped, dormitory-style quarters that the country’s otherwise robust contact tracing system had entirely overlooked (Ratcliffe, 2020).

Older people also have been disparately impacted by COVID-19 and are incentivized to avoid digital scrutiny. As legal scholars have pointed out, the lives of older Americans have been devalued and viewed as expendable throughout the pandemic (Kohn, 2020). The residents of nursing homes and other overcrowded congregate care settings have been the victims of more than half of the COVID-19 fatalities across numerous states due to lack of government regulation. Older Americans may be motivated to opt out of digital data collection platforms due to fear of placement in such a viral incubator or at the bottom of a hospital triage list.

Other stigmatized individuals at high risk for COVID-19 infection who have been subject to criminalization and heightened surveillance because of their status, including sex workers, individuals with substance use disorder, people with HIV, sexual minorities, people who are homeless, individuals with disabilities, and people who are criminal justice-involved, may also be weary of digital tracking due to the possibility that public health authorities will share their data with the police or other government regulators. It is difficult to argue that such concerns are misplaced. The United States does not have in place a health data privacy statute that proscribes public health officials from sharing digital contact tracing data with law enforcement agencies.
It warrants emphasis that promises from public health agencies that they will safeguard such data from law enforcement notwithstanding their lack of legal obligation to do so are insufficient. During the summer of 2020, Singapore instigated widespread use of its digital TraceTogether application by expressly ensuring its citizens that the collected data would be used exclusively for contact tracing. In early January 2021, however, Singapore reneged on that promise by announcing that “[t]he Singapore Police Force is empowered ... to obtain any data, including TraceTogether data, for criminal investigations” (Wamsley, 2021). Even assuming that the United States had laws and policies in place that addressed these law enforcement surveillance concerns, a significant subset of stigmatized and marginalized individuals would nonetheless be excluded from participating in digital contact tracing because they lack access to an adequate mobile device or data plan.

Lessons Learned

There are at least three lessons that can be gleaned from America’s failure to deploy contact tracing in a manner sufficient to stymie the spread of COVID-19.

First, contact tracing cannot succeed without a robust and coordinated public health infrastructure. Before the next pandemic arrives, the United States needs to develop a federal plan that provides resources and funding to enable states to implement widespread, accurate, and timely testing, stand up a public health contact tracing workforce that is adequate to meet the challenge presented, and distribute the technological tools to at-risk populations to empower these groups to participate in digital public health surveillance. The federal government also should facilitate the creation of a digital tracking application for national adoption and use. The use of heterogenous digital tracing application across jurisdictions makes it difficult for those platforms to identify individuals who have been infected by COVID-19 and their contacts.

Second, the United States needs to enact a comprehensive health data privacy law that protects user privacy and, thereby, encourages the mass adoption of digital contact tracing applications during a public health emergency. Such legislation should ensure user privacy by minimizing data collection, permitting the deletion and correction of data, extending to users a privacy right of action, and complying with international data security best practices. It should also respect user autonomy, assure informed, voluntary consent, prohibit discrimination and the dissemination of collected information to non-public health authorities, prescribe the commercial use of collected data, proscribe the sharing of collected data with non-public health government entities, mandate government transparency, and include a sunset provision.

Finally, government officials need to carefully cultivate the trust of the American public generally, and stigmatized and marginalized populations specifically. The enactment of a comprehensive health data privacy law will further this cause, but is not enough. Federal and state policymakers can enhance public trust by embracing the threshold human rights principles of transparency and accountability and expressly combatting misinformation (Davis, 2020). The United States also must adopt public health emergency responses that protect marginalized groups from discrimination and ensure equal access to information, social services and supports, and health care. As the World Health Organization (WHO) has warned, a country’s failure to pay ‘explicit attention to the needs and vulnerabilities faced by [marginalized and stigmatized] groups subjects them to higher risk of infection and undermines the broader [public health emergency] response’ (WHO, 2020).
Recommendations for Action

Federal government:

- Congress should enact a statute that safeguards individuals from the risks that attend to digital contact tracing applications that, at the minimum, ensures user privacy; assures informed, voluntary participation; respects user autonomy; prohibits discrimination and the dissemination of collected information to non-public health authorities; proscribes the commercial use of collected data, mandates government transparency and accuracy, guarantees data security; includes a sunset provision; and extends a private right of action to users.

- In coordination with Congress, the executive branch of the federal government should develop and implement a national response that provides states with the resources and funding to implement accurate, fast, and widespread testing and stand up a robust and adequate contact tracing workforce.

- The executive branch should also adopt a single, well-designed contact tracing application that is user friendly, assists rather than undermines traditional track and trace efforts, and is compliant with the federal legislation outlined above.

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 and has the same features as the federal legislation previously described.

- To ensure that contact tracing apps and processes do not reflect bias or infringe upon civil liberties and human rights, state governments should ensure that contact tracing applications neither (1) disparately burden individuals on the basis of race, ethnicity, nationality, sex, religion, immigration status, LGBTQ status, or disability nor (2) document information that implicates users’ civil liberties or human rights.

- State 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.

- State 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.
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 U.S. 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