PUBLIC HEALTH SURVEILLANCE IN THE CONTEXT OF COVID-19

JENNIFER OLIVA

Partial Transcript of Virtual Grand Rounds Summer Series Lecture[*]

July 31, 2020

PROFESSOR OLIVA: Thank you so much Professor Terry for having me today, and a huge thanks to Director Brittany Kelly for organizing such a fabulous program. It is a privilege to be here. Professor Terry, thank you as well for showcasing junior scholars and giving us so many opportunities throughout the year to present our work.

I am well aware that it is Friday afternoon and I am going to do my very best today to try to make this entertaining. I really look forward to your questions at the end of the presentation because that is when I always learn something new.

Today, we are talking about public health surveillance in the context of COVID-19. My presentation will focus on contact tracing, so let me give you a roadmap for today's discussion. I am going to start out by providing some background on traditional contact tracing, including its genesis, efficacy, and benefits. I will also highlight some of the significant challenges with contact tracing and disease surveillance with a focus on COVID-19 and the current state of track-and-trace in the United States.

I will then explain the various digital track and trace technologies that have been developed or are under development to supplement traditional contact tracing to make the process more effective. I will also point out the strengths and weaknesses that attend to the current technologies that are available in the United States and abroad.

I will then provide a survey of health data privacy laws. One of the themes that I want to emphasize today is that we do not have a federal-level general data protection law in the United States. Therefore, once we start talking about the collection of sensitive health care data outside the traditional health care system, we start to run into huge gaps in the law. I will touch on the California Consumer Privacy Act as well as the recent bills that have been introduced in Congress to protect health data captured by contact tracing applications. I will also give an overview of one of the most misunderstood laws in the United States—the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

I will conclude by discussing the legal recommendations from my recent book chapter, which I derived from the work of a number of scholars who have closely examined the benefits and weaknesses of digital track and trace

---

* *Indiana Health Law Review* and the William S. and Christine S. Hall Center for Law and Health at the Indiana University Robert H. McKinney School of Law give special thanks to Professor Jennifer Oliva for participating in the Virtual Grand Rounds Summer Series and providing her perspective on public health surveillance. Professor Oliva is an Associate Professor of Law at Seton Hall Law.

technology.[1] These scholars include bioethicists, computer scientists, digital technology experts, epidemiologists, as well as health law and privacy scholars. These recommendations envision the implementation of a comprehensive and successful digital contact tracing strategy throughout the United States. After reviewing the recommendations, I look forward to taking your questions. So, let's get started.

We are going to talk about traditional contact tracing first. The gentlemen here on my first slide is the plague doctor, who treated individuals suffering widespread medieval European epidemics. Scholars trace the advent of plague-doctoring to the mid-seventeenth century Western Europe bubonic plague outbreak.

You can see the plague doctor is donning a quite unique outfit, the concept of which is credited to French royal physician Charles de Lorme. The most famous aspect of the plague doctor's costume is the beak-shaped mask. At the time, the dominant theory was that contagions were spread by miasmas—or poisoned air that emanated from organic material such as rotting things or dead bodies. The "bad air" would create an imbalance in a victim's "humors" or bodily fluids and cause the victim to become infected with the plague and fall ill. The purpose of the beak was to protect the plague doctor from these poisonous miasmas. The beak masks that were worn at the time were about six inches long and stuffed with aromatics, such as nosegays, cloves, mint, theriac, and other protective herbs. In short, the beak mask would protect the plague doctor from inhaling pestilential miasma.

The second interesting aspect of the plague doctor's costume is the stake or cane. The stake—which was approximately six feet in length—served as an early social distancing tool, which the doctor used to ensure they stayed far enough away from contagious persons. Miasma theory, of course, has been entirely debunked by germ theory, and we now know that the bubonic plague was caused by *Yersinia pestis* bacteria. The stake, however, is an important symbol in the context of COVID-19 surveillance because we generally view "contacts" as individuals who have been within six feet of an infected individual for approximately fifteen minutes.

Contact tracing is a time-tested public health invention intended to identify and stem the spread of contagious diseases. It is a three-step resource-intensive process. The initial step is for public health workers to accurately identify an infected individual, which is called a "case." The public health workforce then reaches out to that infected individual and interviews them to identify their "contacts"—that is, the people that the interviewee has been in contact with who are at risk of disease exposure.

Modern day case interviews are extensive. Just today, *The New York Times* published an article called "Contact Tracing Is Failing in Many States: Here's

---

1. Jennifer D. Oliva, *Surveillance, Privacy, and App Tracking, in* ASSESSING LEGAL RESPONSES TO COVID-19 40 (Scott Burris et al. eds., 2020), https://static1.squarespace.com/static/5956e16e6b8f5b8c45f1c216/t/5f4d6578225705285562d0f0/1598908033901/COVID19PolicyPlaybook_Aug2020+Full.pdf [https://perma.cc/H8FE-J3NJ].

Why."[2] Among the things the article discusses is the number of questions that contact tracers ask interviewees during contact tracing phone interviews, which can include up to thirty questions. The article points out that contact tracing interviews are often invasive. Some public health departments, for example, begin their interview with an infected individual by asking them where they woke up on the morning of the call or who they slept with the night before. Contact tracers also need to ascertain the identity and contact information of every person that the infected individual has had potentially transmissible contact with over the prior fourteen-day period. These interviews, therefore, are time-consuming and seek very detailed, personal information. As a result, it is critical that the contact tracer is trained to build rapport and trust with case interviewees.

Last but not least, the contact tracer is required to reach out to interviewee's contacts and (1) inform them that they have been exposed to COVID-19; (2) encourage them to get tested and give them information about how to assist with that process; and (3) ask them to quarantine and isolate themselves. The process is iterative and goes on and on from there.

The Johns Hopkins Center for Health Security, the Association of State and Territorial Health Officials ("ASTHO"), and the Centers for Disease Control and Prevention ("CDC") estimate that the United States needs approximately 100,000 trained contact tracers in order to effectively implement conventional COVID-19 contact tracing.[3] A National Public Radio survey of United States public health departments published in late June 2020 found that our contact tracing workforce is at only about 37,000 strong.[4] In other words, we currently do not have even half of the public health workforce in place that we need to conduct effective contact tracing.

I do not point this out to criticize already over-taxed local public health departments. It is difficult and time-consuming to train people to become effective contact tracers in the middle of a surging pandemic driven by a disease that does a lot of its work through asymptomatic transmission.

---

2. Jennifer Steinhauer & Abby Goodnough, *Contact Tracing Is Failing in Many States. Here's Why*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/31/health/covid-contact-tracing-tests.html [https://perma.cc/DKZ5-LYSU].

3. MICHAEL FRASER ET AL., ASS'N OF STATE & TERRITORIAL HEALTH OFFICIALS, A COORDINATED, NATIONAL APPROACH TO SCALING PUBLIC HEALTH CAPACITY FOR CONTACT TRACING AND DISEASE CONTROL 4 (2020), https://www.astho.org/COVID-19/A-National-Approach-for-Contact-Tracing/ [https://perma.cc/9HKR-3VGC]; Tanya Albery Henry, *Experts: Here's How Many More Contact Tracers U.S. Needs*, AMA (July 30, 2020), https://www.ama-assn.org/delivering-care/public-health/experts-here-s-how-many-more-contact-tracers-us-needs [https://perma.cc/ZC76-C43R].

4. Selena Simmons-Duffin, *As States Reopen, Do They Have the Workforce They Need to Stop Coronavirus Outbreaks*, NPR (June 18, 2020), https://www.npr.org/sections/health-shots/2020/06/18/879787448/as-states-reopen-do-they-have-the-workforce-they-need-to-stop-coronavirus-outbre [https://perma.cc/G3PY-XE5X].

New York City has long had a fifty-person contact tracing team.[5] In response to COVID-19, however, the City ramped up its new "Test and Trace Corps" from fifty to 3,000 tracers in two weeks at the beginning of June 2020. As the media has detailed, this rapid attempt to bolster the force has been challenging and riddled with problems. The City's forty-five minute, sixteen-step questionnaire, which begins with questions about race and sexual orientation and fails to even broach inquiries about the interviewee's contact until step eleven, is particularly concerning.

The benefits of traditional contact tracing are well-documented in the public health literature. Contact tracing has proven effective at detecting and mitigating the spread of contagious diseases. Also, when contact tracers do build a rapport with their interviewees, they can assist infected individuals to obtain social services and other resources that facilitate health-enhancing behaviors and make it easier to isolate or quarantine for up to two weeks.

Massachusetts has been lauded for its contact tracing program because the Commonwealth's contact tracers start their interviews by asking interviewees whether they need assistance, such as help procuring groceries or medications, to facilitate quarantine and isolation. It appears that several of Massachusetts' 351 public health departments have adopted this approach and have been successful at building rapport and trust quickly with interviewees by offering help at the front end of the interview.

Traditional contact tracing can promote economic recovery, and thereby reduce widespread economic anxiety and suffering. It can also facilitate the protection of vulnerable populations that are at a higher risk of contracting COVID-19 and more likely to experience an adverse health outcome attributable to infection or—worse—succumb to the disease.

Contact tracing, of course, has its detractors. It has been characterized as slow, passive, and riddled with holes. This is because contact tracing relies on two very important things: honesty and human memory. As already mentioned, contact tracers attempt to get interviewees to cooperate and honestly respond to very personal questions, such as who the interviewee had intimate contact with over a two-week period. Moreover, even assuming the interviewee trusts the tracer and desires to communicate personal information honestly, the interviewee is nonetheless limited by the constraints of human memory. With COVID-19, which spreads from infected but often asymptomatic persons to others, it is very difficult for human beings to remember everyone they have had contact with or stood within six feet of for ten to fifteen minutes over a fourteen-day period. To try to mitigate such memory limitations, traditional contact tracers often ask interviewees to reference their phones and calendars to refresh their recollection. Needless to say, traditional contact tracing is a time-intensive and imperfect process beset by the fallibility of human memory.

A recent COVID-19 spreading event in my home state of New Jersey helps

---

5. Sharon Otterman, *City Praises Contact-Tracing Program. Workers Call Rollout a 'Disaster*,*'* N.Y. TIMES (July 29, 2020), https://www.nytimes.com/2020/07/29/nyregion/new-york-contact-tracing.html [https://perma.cc/8969-GWZE].

us put the challenges that attend to traditional contact tracing in perspective. On July 11, 2020, approximately 100 teenagers between the ages of fifteen to nineteen attended a large house party in Middletown, New Jersey, which is in Monmouth Country where the Governor of New Jersey lives.[6] Shortly thereafter, more than twenty of those teenagers tested positive for COVID-19 and the Middletown Health Department quickly realized that it had to attempt to contain community transmission of the virus. In an attempt to do so, the Middletown Health Department began to reach out to the teenagers who had attended the party as well as their parents.

The contact tracers, however, met widespread resistance. Many of the parents and teenagers refused to take the Health Department's calls or answer any questions. This demonstrates the challenges that public health departments and their contact tracers face in the context of a problematic spreading event. The Middletown teenagers did not want to tell their parents that they had been at an indoor party in the middle of the pandemic where they may or may not have been drinking alcohol or taking part in other activities. And, their parents did not want the teenagers targeted or investigated by the township, county, or state. I looked at the status of this cluster this morning and there are now more than fifty teenagers who have tested positive for COVID-19 linked to that single July 11 house party.[7]

While trust in the public health system is a considerable problem, the biggest obstacle to effective contact tracing is the country's lack of accurate, widespread, and timely COVID-19 testing. As things currently stand in the United States, state and local government entities are responsible for testing and contact tracing. There remain far too few tests and the lag between tests and the issuance of test results remains too wide. In numerous states, symptomatic individuals have to wait up to seven to nine days to get their COVID-19 test results. I cannot emphasize enough that it is near-impossible to control or mitigate a contagion that spreads through asymptomatic transmission for days without timely and accurate testing. The current state of COVID-19 testing undermines the hope that contact tracing can succeed.

I am not an infectious disease expert by any stretch of the imagination. In fact, pre-COVID-19, I limited my examination of the law and policy that attend to contagious diseases and infectious diseases that are co-morbid with substance use disorder. Those diseases, like syphilis or human immunodeficiency virus ("HIV"), are easier to track and trace because they do not spread from person to person silently through the air. COVID-19 transmission is an entirely different situation. The fact that we do not have robust testing in the United States is the

---

6. Jorge Fitz-Gibbon, *COVID-19 Cluster Linked to NJ House Party, Parents Not Cooperating with Tracers*, N.Y. POST (July 23, 2020), https://nypost.com/2020/07/23/nj-party-leads-to-coronavirus-cluster-parents-wont-cooperate/ [https://perma.cc/9SC8-6CGN].

7. Carly Baldwin, *65 New COVID Cases in Middletown, Nearly All in Teens 15-19*, PATCH (July 27, 2020), https://patch.com/new-jersey/middletown-nj/65-new-covid-cases-middletown-nearly-all-teens-15-19 [https://perma.cc/8T3G-YB4Q].

Achilles heel for traditional contact tracing, and it is not a problem that can be remedied by digital applications.

A popular media narrative that emerged this spring is the notion that digital contact tracing would save us from the shortcomings of traditional contact tracing. As the story goes, digital contact tracing will be particularly useful in the context of COVID-19 because it does not depend on human memory or honesty. Instead, it uses surveillance technology to pinpoint "contacts." Digital track-and-trace, therefore, will provide the public health workforce with more detailed and precise information about potential asymptomatic transmission and do so more quickly.

Media accounts circa March and April of 2020 made it seem inevitable that the United States would adopt widespread digital contact tracing. American technology behemoths, Google and Apple, announced that they were joining forces to develop exposure notification digital application programming interfaces ("APIs") that work on both Android and Mac OS smartphones. These applications use smartphone short-range Bluetooth signals to anonymously keep track of phone proximity and then send alerts to users who have potentially been exposed to someone who has tested positive for COVID-19.

Is this technology an improvement on traditional contact tracing? The general consensus is a resounding yes. Digital contact tracing is more comprehensive than traditional tracing because it tracks proximity between application users at all times so long as those users have their phones on and have enabled the application. Assume you keep your phone or your digital device on your person at all times and have downloaded a digital tracking application. You no longer need to be honest with contact tracers and divulge sensitive information to strangers. You also do not need to have an infallible memory. Digital contact tracing is much cheaper and faster than traditional tracing because it avoids the need to conduct time-intensive interviews and build rapport with skeptical interviewees. As a result, digital contact tracing has been heralded as a huge improvement in the traditional process.

Digital contact tracing, however, also suffers serious flaws. First, and as already mentioned, digital track and trace technology cannot function effectively without widespread and accurate testing in place. Traditional contact tracing must discern when someone is infected in a timely manner in order to mitigate spread. Digital tracing applications must be able to do the same. This is because tracing applications do not send notifications to contacts unless and until there is some indication that an application user is positive. Given the asymptomatic contagious period that attends to COVID-19, our lack of widespread, timely testing undermines both traditional and digital contact tracing.

Second, and unlike traditional contact tracing, individuals who either do not have access to a smartphone or lack a data plan needed to support track and trace applications are excluded from digital contact tracing. Moreover, the Google and Apple APIs rely on Bluetooth technology that is only available on newer devices. It is possible, therefore, that even someone like my mother—who has a very old smartphone and refuses to get a new one—would be excluded from using the Google and Apple digital tracing applications. As a result, digital contact tracing can supplement—but not entirely supplant—traditional contact tracing. Some

people simply do not have access to the necessary technology or the technical expertise to participate in traditional tracing, while others may prefer to talk to a human being with whom they can build rapport and trust.

Third, although digital contact tracing requires less individual cooperation than traditional tracing, it still requires some cooperation. Let us revisit the earlier example with the New Jersey teenagers. The individuals who attended the party could have eluded digital contact tracing just as effectively as they dodged the Middletown health authorities by simply disabling the tracing applications on their phones during the house party or leaving their phones in their cars. So, there are limits to digital tracing in particular situations involving even savvy smartphone users who have the latest technology and who want to avoid detection or surveillance.

Digital contact tracing also raises heightened privacy and civil liberties concerns relative to traditional contact tracing. Traditional tracing is very invasive. Traditional contact tracers ask a myriad of questions about individual conduct and associations that interviewees may not want to answer and that implicate others. That, however, pales in comparison to digital contact tracing, which either tracks users' movements or their proximity to others 24/7.

There are two primary types of digital contact tracing applications, one of which is preferred to the other on privacy and efficacy grounds. The first type of digital contact tracing relies on "location applications." These apps use global positioning service technology or cell site location information to pinpoint the application user's location on planet Earth. Location applications track your geolocation when you go into a store to shop, walk-in or out of your home, or drive on the Garden State Parkway.

The second type of digital contact tracing is driven by proximity technology. These applications do not track the user's geolocation or whereabouts on planet Earth. Instead, they use Bluetooth Low Energy signals to track the distance between the user's digital device—such as their phone or tablet—and other users' digital devices, as well as the time that elapses once two users' devices, are proximate to one another for a period of time that might trigger exposure.

There are significant differences between location and proximity applications. Location application data uses global positioning service ("GPS") and cell site location information ("CSLI") technology. CSLI consists of pings that our smartphones are constantly making to cellular towers to give us cell phone access. Location applications, therefore, collect a lot of personal data about their users' whereabouts or movements.

They are nonetheless disfavored vis-à-vis proximity applications. This is because CSLI often is not sensitive enough, particularly in rural and suburban areas, to actually pinpoint whether a user has been close enough to another person—say within six feet—for a long enough period of time—ten to fifteen minutes—to trigger a contact. In other words, while location applications can be quite revealing about where a user has traveled and about a user's activities (e.g., whether a user has attended a church or a political rally or sought services at an abortion clinic), they are not particularly useful in identifying other individuals with whom the user has had contact, especially in rural and suburban

communities where there are not as many satellites to triangulate a user's precise geolocation. In sum, location applications are accurate enough to reveal sensitive data, but often not accurate enough for reliable digital disease tracing.

Proximity applications do not rely on either GPS or CSLI data. Instead, they use advanced low-level energy Bluetooth technology that is available on newer smart devices. The Bluetooth signal strength from application users' phones measures the distance between the users and tracks their time proximate to each other. For example, if Professor Terry and I are within six feet of one another for ten to fifteen minutes, our Bluetooth proximity applications on our phones are going to capture and log that interaction. If one of us tests positive for COVID-19 within two weeks of our interaction, the application will send the other an exposure notification. Proximity applications are preferred over location applications on privacy and effectiveness grounds because they are superior at capturing meaningful contacts but do not divulge a user's sensitive activities or associations (such as whether a user attended a Scientology church service or a political rally last weekend).

There is considerable variation as to how proximity applications work once they log a contact. I am going to over-generalize here, but I will try to frame up these variations by separating the major data collection approaches that attend to proximity applications into three broad categories: (1) centralized data collection; (2) semi-decentralized data collection; and (3) decentralized data collection. Let's do a quick overview of each category.

Singapore's "TraceTogether" program provides a paradigm example of the centralized or top-down data collection approach. The "TraceTogether" program trusts a centralized authority—the Singapore Ministry of Health—to collect user contact information, including users' phone numbers, email addresses, and physical addresses. Let's go back to my previous example where Professor Terry and I both have a Bluetooth proximity application active on our phones and those applications logged our potential exposure contact. If we were on the Singapore platform, pertinent information on our phones—including our unique user identifiers and contact information—would be uploaded from our phones into a centralized database operated and controlled by the Singapore Ministry of Health.

If I then test positive for COVID-19, my positive test goes into the system so that Professor Terry and all of my other contacts can be notified. The Department of Health thereafter reaches out to Professor Terry and those other contacts to ensure that they are aware of the potential exposure, can isolate, and get tested. In Singapore, if a public health department is notified that someone has tested positive, the department is responsible for uploading that information into the database. Individuals who test positive can also upload that information to the centralized database themselves. The centralized database, therefore, collects a lot of individual user information.

There are digital trace-and-trace platform options, however, that take a less centralized and more middle-ground approach by delegating more agency to individual users. In these systems, the central authority has less access to sensitive user data. The user has more autonomy to decide when and what to upload to the database and more uploaded information is de-identified. So, in our ongoing hypothetical, once I test positive in a semi-decentralized system, the application

uploads my phone's unique user identification to the centralized database but not my name, email, or residential address. The semi-decentralized database then triggers an automatic ping or exposure alert to my contacts, including Professor Terry, instead of contacting me or Professor Terry directly because the system does not have any of our identifiable contact information. The reason why these systems are deemed semi-decentralized instead of decentralized is because de-identified information is uploaded and shared with a central database automatically.

The final category of proximity application data collection is the decentralized notification platform. This is the type of system that Google and Apple collaborated to develop with the aim of maximizing user privacy. In this system, there is no central authority that maintains or has access to a centralized database. Instead, there is a public database that collects and broadcasts unique user identifiers. This system neither collects nor stores any personally identifiable information.

Such decentralized systems do alleviate many—but not all—of the privacy concerns raised by COVID-19 digital contact tracing. This is because it is likely impossible to truly de-identify any data in modern times. Experts have proved exceptionally adept at re-identifying purportedly de-identified data because so much of our personal data is already publicly available. It is an open question whether these lingering re-identification issues can be ameliorated with robust encryption and other security safeguards.

Proximity track and trace technology platforms face additional challenges in the United States. First, their ability to succeed hinges on their widespread adoption which, in turn, hinges on widespread public trust of the platform and its underlying technology as well as the government actors involved. The conventional wisdom is that we would need 80% of all people who have smartphones in the U.S. to adopt and use proximity contact tracking applications to mitigate the spread of COVID-19. This means that nearly 60% of the American public would have to download and use these applications.

Given the widespread mistrust in these applications that currently exist in the United States, however, achieving a 60% proximity application user rate seems unlikely anytime soon. Polls have shown that more than half of Americans either do not have access to technology that would permit them to participate in digital contact tracing or simply will not use the applications if they do.[8] These poll results are quite believable if you compare them to the participation information that we have gleaned over the months about Americans' willingness to communicate with traditional contact tracers. When New York City's contact tracers started reaching out by phone to individuals who had contracted COVID-19 in June 2020, only 42% of those people would provide the tracers with even

---

8. Reuters Staff, *Most Americans Cannot or Will Not Use COVID-19 Contact Tracing Apps: Poll*, REUTERS (Apr. 29, 2020), https://www.reuters.com/article/us-health-coronavirus-tech-tracing/most-americans-cannot-or-will-not-use-covid-19-contact-tracing-apps-poll-idUSKBN22B2TO [https://perma.cc/AQS2-5TM8].

a single contact. And only 58% to 60% bothered to answer their phones at all.

The State of Maryland has experienced even worse results, reporting that a mere 25% of the individuals phoned by contact tracers take the call. Even more dire, Florida's Miami-Dade Public Health Department has only had success reaching 18% of individuals who have contracted COVID-19. Although the United States may never reach efficacious rates of digital contact tracing participation, it warrants noting that every contact traced potentially saves lives.

There are, however, at least two additional problems with digital contact tracing: over-inclusivity and under-inclusivity. First, Bluetooth proximity technology can lead to false positive exposure notifications because of its inability to discern if there are barriers between contacts that significantly lower the risk of COVID-19 transmission. The technology, for example, fails to account for the fact that there may well be walls in between people who are six feet apart. If you live in a New York City high-rise building and you are only separated from a neighbor by a shared wall, the technology could potentially count you as an exposure risk to your neighbor even though you and your neighbor live in separate apartments and have had no in-person contact. Also, assume Professor Terry and I are driving on the highway in parallel lanes and we both stop at a red light. Bluetooth technology would not discern that we were in separate vehicles with our windows up and, therefore, pose little to no exposure risk to one another. Bluetooth proximity applications, therefore, run the risk of constantly over-notifying people notwithstanding minimal chance of exposure. The technology also cannot ascertain whether potential contacts are wearing personal protective gear—such as a mask or a face shield—when they are proximate to one another. It would not count, for example, for someone who was wearing a hazmat suit. This runs the risk of exposure notification fatigue for health care and other essential workers who wear PPE as a matter of course and have a high number of daily contacts.

Perhaps even more problematic is the fact that the technology is under-inclusive and therefore, produces false negatives. As I have already discussed, the proximity contact tracking applications only work if a user has a newer device, an adequate data plan, and has downloaded and activated the application. But even that is not enough. The user also has to carry the device on their person at all times in order for the application to be effective. Imagine going to a relative's home and leaving your phone in your coat that you hang on a hook near the front entrance of the residence. Your relative's phone is charging on a stand in her bedroom during your visit. The two of you sit within six feet of one another for approximately two hours catching up. Your relative later tests positive for COVID-19, but you never receive an exposure notification notwithstanding your extensive proximity to her because your phones were never within six feet of one another. Proximity applications treat your phone as a proxy for your body. As a result, whenever a person's phone turns out to be a poor proxy, these applications run a significant risk of under-inclusive exposure notification.

The other thing I want to point out is that Bluetooth low-energy signaling is constant work for your mobile device and, therefore, drains the device's battery quickly. So, yet another concern that attends to this technology is whether it is even possible for users to keep their phones operating throughout the day if they

are running the application in the background. At some point, users are going to be hyper-incentivized to disable the application so that they can preserve the battery on their devices to use those devices for other purposes.

So much for the imminently positive news about the technology. An ancillary interesting issue is whether there has been widespread adoption of digital contact tracing technology outside the United States. As it turns out, there has been a relatively low uptake of digital contact tracing globally. There are, however, at least a few countries that have adopted the technology with some success.

As previously mentioned, Singapore adopted its centralized "TraceTogether" application in March 2020 and Switzerland became the first country to release the decentralized Google-Apple exposure notification application in May 2020. Ireland and Germany also have launched digital contact tracing applications with open-source codes that anyone can inspect, and those countries have realized relatively high application adoption rates with their citizens.

Taiwan has also been lauded for its successful digital contact tracing by involving its citizens in the development and deployment of the surveillance platforms.[9] In all fairness, Taiwan may be a cultural democratic outlier in this context. This is because the country suffered a severe acute respiratory syndrome ("SARS") epidemic in 2003 and, therefore, was culturally poised to aggressively contain and mitigate the spread of COVID-19. It is impossible to fairly assess popular sentiment toward surveillance technology without accounting for a nation's collectivist versus individualist cultural leanings as well as its recent history with contagion.

While Ireland and Switzerland appear to be succeeding with digital COVID-19 surveillance, other western nations have realized opposite results. Norway and the United Kingdom, for example, adopted but then quickly abandoned the use of digital track and track technology due to low uptake. The United States also has had little success with either adoption or uptake of COVID-19 digital surveillance. In a recent survey, only four states' public health authorities indicated that they intend to use the Google or Apple exposure notification application. An expert at the Bergman Klein Center at Harvard University recently announced that he does not believe that digital contact tracing will be widely and successfully adopted in the United States unless things change dramatically in the near future.

I would submit that it nonetheless is important to understand the technology given our potential to be digitally tracked and traced while at work or at school, even if the states do not adopt the technology. In the meantime, I would recommend to those that are interested in national and global developments regarding digital contact tracing to visit the Massachusetts Institute of Technology's COVID-19 digital contact application tracker, which you can access online by searching for "MIT Technology Review COVID Tracing

---

9. Andreas Kluth, *If We Must Build a Surveillance State, Let's Do It Properly*, BLOOMBERG (Apr. 22, 2020), https://www.bloomberg.com/opinion/articles/2020-04-22/taiwan-offers-the-best-model-for-coronavirus-data-tracking [https://perma.cc/8ME4-EYY2].

Tracker."

Let's transition now to an overview of the legal powers that attend to government actors during public health emergencies in the United States and the American health data privacy legal regime. It is the states—and not the federal government—that have the most power under the United States Constitution during a public health emergency. This is because, while the federal government is confined by its enumerated powers, the Tenth Amendment to the Constitution broadly reserves the police—or public health and safety—power to the states. The federal government's public health and safety powers traditionally come from its Commerce Clause and Tax & Spending Clause authority. So, the federal government's primary role in a pandemic is to declare national emergencies, provide the states with resources and funding to mitigate the contagion, and serve as the source of national coordination.

The Supreme Court affirmed the breadth and scope of the police powers that are reserved to the states to protect public health from the spread of contagious diseases in a pair of cases decided in the early 20th Century. The first, and probably more famous of those cases that warrant discussion, is *Jacobson v. Massachusetts*, which was decided by the United States Supreme Court in 1905.[10] That case involved a Cambridge, Massachusetts pastor, Henning Jacobson, who refused to be vaccinated in violation of Cambridge's mandatory vaccination ordinance. Jacobson argued that the compulsory vaccination law was unreasonable, arbitrary, and capricious and, therefore, ran afoul of his Fourteenth Amendment rights to due process and equal protection. The Supreme Court disagreed and broadly deferred to Cambridge's power to protect public health in upholding the compulsory vaccination law.

The second important seminal public health powers case that the Supreme Court decided just before it issued its decision in *Jacobson* is *Compagnie Francaise de Navigation a Vapeur v. Board of Health of Louisiana*.[11] In the early 1900s, a ship from Europe arrived at the Port of New Orleans while the City of New Orleans was in the midst of a yellow fever outbreak. New Orleans public health officials tested the ship's passengers for yellow fever, and no one was carrying the disease. Those officials nonetheless refused to permit the passengers to disembark from the boat and enter New Orleans. The question in the case was whether the New Orleans Board of Health had the authority to exclude non-infected individuals from entering the city. The Supreme Court held that it did on the theory that the City had broad *cordon sanitaire* public health powers, which permitted it to exclude from its jurisdiction non-infected individuals to prevent them from becoming disease vectors. The takeaway here is that, while not unlimited, the public health powers reserved to the states are vast. As Professors Larry Gostin and Lindsay Wiley have explained, a state exercise of power to protect health and safety is subject to five balancing principles derived from the *Jacobson* decision—public health necessity, reasonable means, proportionality,

---

10. Jacobson v. Massachusetts, 197 U.S. 11 (1905).

11. Compagnie Francaise de Navigation a Vapeur v. La. State Bd. of Health, 186 U.S. 380 (1902).

harm avoidance, and fairness.[12]

So, first, the state must establish that there is a real public health threat. If there is no public threat, the state has no business restricting individual liberties. Second, and even if there is an actual public health threat, government intervention must be calibrated to address that threat. The state's response must be designed to reasonably mitigate the spread of the disease. Third, the state's exercise of its public health powers must be proportional to the public health threat. The burden that the state places on individuals cannot be wholly disproportionate to the expected benefits of those burdens.

The fourth *Jacobson* principle is harm avoidance. That is to say that the state's control measures should not impose a public health harm on individuals. Under this principle, Pastor Jacobson could have won his case if he had established that taking the vaccine would have harmed his health.

Last but not least, is the principle of fairness, which demands that the state exercise its public health authority equitably and not in a manner that is arbitrary or discriminatory. The federal courts established the principle of fairness in this context in *Jew Ho v. Williamson*.[13] *Jew Ho* involved the City of San Francisco's decision to place on quarantine only its Chinatown neighborhood despite a city-wide outbreak of bubonic plague. Mr. Ho was a Chinatown merchant who challenged the quarantine on the grounds that it was racially discriminatory and irrationally targeted people of Chinese descent. The United States District Court for the Northern District of California agreed with Mr. Ho and struck down the quarantine as racist, arbitrary, or unreasonable and, thereby, established that it was unconstitutional for a state to exercise its police powers inequitably.

The importance of the fairness principle is highlighted in the COVID-19 religion cases that have been appealed to the United States Supreme Court over the last several months. As a general rule, these cases involve a religious group's attempt to enjoin state COVID-19 orders that restrict the group's right to assemble on due process and equal protection grounds. The Court has thus far rejected those challenges. For example, in *South Bay Pentecostal Church v. Newsome*, religious applicants challenged California Governor Gavin Newsome's order limiting attendance at places of worship to 25% of building capacity or 100 attendees.[14] The Supreme Court refused to enjoin Governor Newsome's order because it applied its COVID-19 restrictions equally to secular and non-secular indoor gatherings.

The United States Court of Appeals for the Sixth Circuit, on the other hand, granted injunctive relief to a Kentucky church this spring in *Maryville Baptist Church v. Beshear*.[15] In that case, the church challenged the Kentucky governor's order that prohibited church members from attending drive-up religious services

---

12. LAWRENCE O. GOSTIN & LINDSAY F. WILEY, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 125-26 (3d ed. 2016).

13. Jew Ho v. Williamson, 103 F. 10 (N.D. Cal. 1900).

14. S. Bay United Pentecostal Church v. Newsom, 140 S. Ct. 1613 (2020).

15. Maryville Baptist Church, Inc. v. Beshear, 957 F.3d 610 (6th Cir. 2020).

even if the church members complied with the social distancing and capacity limitations that applied to secular activities. The church argued that the order was unconstitutional because it permitted Kentuckians to go to drive-in theaters but proscribed them from attending drive-in religious ceremonies. The Sixth Circuit agreed with the church and enjoined the governor's order on fairness principles.

As things currently stand, it appears that states do have the authority to conduct digital contact tracing to stymie the spread of COVID-19 so long as such tracking comports with the five public health balancing principles. The open question is whether individuals have privacy rights that might place limitations on such digital surveillance.

There are at least two sources of constitutional privacy rights that the Courts have recognized. First, the Supreme Court identified a Fourteenth Amendment qualified right to informational privacy in *Whalen v. Roe*.[16] The holding in *Whalen* teaches that individuals have a right to informational privacy that must be balanced against the state's need to protect the public health. The Supreme Court has also recognized that individuals have a reasonable expectation of privacy in their sensitive health data under the Fourth Amendment to the Constitution. For example, the Court held in *Ferguson v. City of Charleston* that a state hospital violated patients' Fourth Amendment reasonable expectations of privacy by sharing the results of their diagnostic tests with non-medical personnel, including law enforcement.[17]

The Court recently decided an important Fourth Amendment privacy case, *Carpenter v. United States*, that might impact the scope of constitutional health data privacy protection going forward.[18] Prior to the *Carpenter* decision, the general rule was that an individual who voluntarily shares their health care data with a third party—who, in turn, shares that information with a government agency—has waived their right to raise a Fourth Amendment privacy claim. In *Carpenter*, law enforcement had obtained the petitioner's cell-site location data—which revealed his pertinent whereabouts and movements during the time at issue—from the petitioner's wireless carrier without his consent and without a warrant. The Court rejected the government's claim that Carpenter had waived his right to raise a Fourth Amendment claim and held that law enforcement was required to obtain a warrant to conduct such CSLI surveillance over a period of weeks and months. The *Carpenter* decision, therefore, has serious legal implications for digital location contact tracing applications.

There are nonetheless numerous Fourth Amendment exceptions to the warrant requirement that limit an individual's reasonable expectation of privacy. The government, for example, can conduct warrantless searches at the border—which is expansively defined under American law. And, there are other administrative and special needs doctrines that can undermine Fourth Amendment protection of sensitive data. Moreover, private actors and entities that collect health data for digital contact tracing purposes are not subject to these

16. Whalen v. Roe, 429 U.S. 589, 603-06 (1977).

17. Ferguson v. City of Charleston, 532 U.S. 67, 86 (2001).

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

constitutional constraints.

So, that brings us to a discussion about potential statutory privacy protections. HIPAA is a federal statute that is largely viewed as synonymous with health data privacy. If COVID-19 has taught us anything about health care law, it is that HIPAA is one of the most misunderstood laws in the United States. Since the inception of the pandemic, individuals have created Twitter and other social media accounts dedicated to exposing the myriad misconceptions that Americans have about HIPAA. So, let me attempt to clear some of those misconceptions about the law.

HIPAA only applies to a narrow set of covered entities in the traditional health care system, including health care providers, health care insurance companies, health care clearinghouses, and their business associates. HIPAA does not apply to employers or third-party application creators or operators, such as Google or Apple. In addition, HIPAA only applies to very particular health information. Specifically, the statute only proscribes covered entities from disclosing individually identifying health care information, which the HIPAA privacy rule calls "protected health information" ("PHI"). Health care data that is "de-identified," therefore, is not protected from disclosure by HIPAA.

HIPAA also includes a dozen "public policy" exceptions that permit even covered entities to disclose PHI in certain circumstances to certain other entities. These exceptions permit covered entities to disclose PHI for, among other things, health oversight activities, specialized government functions, law enforcement purposes, research activities, as well as to mitigate or avoid serious threats to public health and safety. HIPAA's privacy scheme also precludes individuals from vindicating their rights even when the statute has been violated. The only entity that can enforce HIPAA is the Department of Health and Human Services' Office of Civil Rights ("OCR"). OCR recently announced that it will exercise its enforcement discretion during the pandemic and not enforce certain HIPAA violations in certain circumstances. In sum, HIPAA requires a very narrow set of entities to protect individually identifying health information subject to a broad swath of exceptions. There is no reason to believe that HIPAA is going to provide any privacy protections in the context of contact tracking so long as the states delegate their COVID-19 digital tracking functions to a state agency that is not covered by HIPAA.

States also have their own privacy protections, some of which are much more robust than federal protections. There are a small number of states, for example, that have expressly recognized a right to health care data privacy in their constitutions. Every state also has enacted a consumer protection statute that provides variable privacy protections. California recently enacted the California Consumer Protection Act ("CCPA"), for example, which is the most comprehensive state-level data privacy scheme in the United States. The CCPA extends to consumers, among other things, the right to correct and delete their data, the right to opt-out of data collection schemes, and the right to privately enforce the statute. The CCPA, however, exempts from its protections HIPAA-covered entities.

Recognizing that the collection and storage of sensitive health care

information in the context of digital contact tracing is unlikely to be protected by federal law, Congress has proposed at least three statutes since April 2020 that are designed to fill the gap. On June 1, 2020, for example, two senators introduced the Exposure Notification Privacy Act ("ENPA"), which aims to provide Americans control over data collected by digital track and trace applications. As currently drafted, the ENPA requires digital contact tracing application operators to collaborate with state public health authorities, obtain consent from enrolled users, permit users to withdraw such consent, and permit users to request data deletion. The statute also limits data collection to that which is minimally necessary to implement the application and proscribes operators from using the data for commercial purposes. The ENPA does not, however, extend a private right of action to individuals to vindicate their statutory rights.

I see that our time is running short. I want to conclude by pointing out that my book chapter addresses all of the topics that we have discussed today pertinent to contact tracing as well as proposes a list of recommendations to state and federal governments that aim to address the significant privacy concerns raised by digital contact tracing. Those recommendations contend that any state or federal legislation that is enacted to extend privacy protection to digital contact tracing application users should, among other things: (1) minimize the data collected; (2) permit users to delete and correct their data; (3) assure informed, voluntary participation; (4) respect user autonomy; (5) prohibit discrimination and the dissemination of collected information to non-health authorities; (6) proscribe the commercial use of collected data; (7) mandate government transparency and accuracy; (8) guarantee data security; (9) include a sunset provision; and (10) extend to users a private right of action.