Antitrust, Vol. 35, No. 1, Fall 2020.

Contact Tracing: Strategies and Issues for Balancing Public Health Demands and Privacy Concerns

BY ROBERT CATTANACH AND NUR IBRAHIM

PUBLIC HEALTH EXPERTS AGREE THAT until a vaccine is developed, the key tools for tackling the spread of COVID-19 require a robust testing model and effective contact tracing of new infections.[1] This need led to the rapid development of new tracing technologies that launched before there was an opportunity to vet them fully. We now have a wave of smartphone apps that can track an individual's movement, notify whomever they have met, register their symptoms, and monitor their health.

This information can be invaluable in combating the spread of the disease. If used by a large enough segment of the population, it could enable public health authorities to locate and isolate potentially infected individuals. The question posed, however, is at what cost to an individual's right to privacy? Like much in the fight against COVID-19—quarantining, wearing a mask, and shutdown orders—there is a sacrifice of individual civil liberties for the greater public good. While that trade off may be essential to get us through this pandemic, these potentially extraordinary intrusions into our private lives may set a concerning precedent for future compromises of individual liberties, whether by mandatory government edict or "voluntary" adoption.

The purpose of this article is to assess the early experiences with various forms of digital contact tracing, identify consequences to civil liberties, discuss the trade-offs between emerging public and private initiatives—including potential antitrust concerns—and address how to protect the public health without unacceptably compromising our civil liberties. We will explore the variety of approaches using smartphone apps around the world, assess how effective, and intrusive, some of these technologies are, and offer considerations for evaluating the optimal balance.

Robert Cattanach is a partner at Dorsey & Whitney LLP, and practices in the areas of cybersecurity and privacy. He was Editor-in-Chief of the Sedona Conference's recently published Incident Response Guide. *Nur Ibrahim is an associate at Dorsey & Whitney LLP, and practices in the Regulatory Affairs group.*

Technology Advantages and Limitations

Contact-tracing apps were developed using two widely available technologies: Bluetooth and GPS. Bluetooth works by sending radio messages to announce the availability of a device to pair with applications running on another Bluetooth enabled device.[2] Bluetooth apps will keep track of when the user's phone sends out a Bluetooth announcement. If that individual tests positive, determining whose phone connected with those messages will provide the baseline for the contact tracing.[3] Bluetooth based apps have been likened to a virtual "handshake" because its markers are designed to determine with whom you came into contact. In contrast, GPS-based systems can track where the potentially infected user has been, and at what time, and can then match up other users whose devices were at the same location during the same time period.[4] This location data allows tracking of potential outbreaks or hotspots.[5]

Both technologies are limited in their ability to properly assess risk, such as whether there was actual contact rather than just proximity (radio waves can travel through walls, but the virus cannot). GPS tends to be less precise, and Bluetooth signals can strengthen with distance due to reflection off metal surfaces.[6] These limitations may reduce the effectiveness of this technology, and may create a false sense of security if individuals never receive an alert about potential exposures, or desensitize people who receive too many.[7] Perhaps most importantly for purposes of this article, the Bluetooth markers likely do a better job protecting privacy than does the GPS technology, since Bluetooth, by itself, does not transmit location data to any central clearinghouse, and therefore does not involve location surveillance.[8] Ultimately, governments and individuals will have to decide whether the compromise in reliability of the Bluetooth approach is worth the enhanced privacy protection.

How the data will be maintained presents additional concerns. As cell phone apps collect data it is either stored at remote centralized servers or on the users' phones. Apps that use a centralized server will typically be able to access the phone IDs of an infected person's contacts to verify that the correct people are receiving notifications of potential exposure once the user reports symptoms or tests positive. In the decentralized app approach, however, health departments only learn about people who actually respond to an alert from their app, and have no way of determining if other individuals were exposed who did not install and activate the app, or how many notified people failed to respond to the notification, and therefore might not be known to health authorities.[9] Use of a centralized server therefore raises concerns about the potential to misuse the data, whereas the decentralized model likely will be less effective for public health officials since it relies on users' voluntary installation and use.

International Approaches: The Experience in Asia, Australia, and Israel

Contact tracing has been instrumental in slowing the spread of COVID-19 in certain countries in East Asia. South Korea was among the first to institute a mobile contact-tracing app to monitor the movements of confirmed COVID-19 patients, building upon its government's existing comprehensive surveillance efforts, which already gather mobile GPS stamps, camera records, and credit card transactions.[10] The app, Corona 100m, collects government surveillance data and shows the date of a diagnosis, nationality, age, gender and where the person visited.[11] Users are alerted when an individual comes into close proximity to a location visited by an infected person.[12] Contact tracing has been credited as an important component of the country's success in quickly flattening the curve of cases[13]—although it is worth noting that South Korea may be facing an unexpected spike in the spread.[14] Many other countries, however, have been hesitant to follow South Korea's example over concerns that it is too intrusive.

China also embraced a very aggressive approach to contact tracing. For individuals wishing to travel outside of their home, local governments across the country deployed an app that determines how much freedom of movement any individual should have throughout society at large. Local governments created a database and health codes that were integrated into two widely popular apps for their technology, WeChat and Alipay.[15] The Alipay Health Code app was launched in the city of Hangzhou as a project by the local government and Ant Financial. When individuals initiate the app, they are required to enter certain personal information, which generates a color-coded QR code to determine how restricted the individual's movements should be. The QR-codes essentially act as an ever-present passport to enter and move about the city.

There is little transparency into what underlying factors determine how an individual is classified, causing confusion and some resentment of the program. Data is sent to a central server that constantly tracks an individual's whereabouts. Since the application was developed in conjunction with law enforcement, user location, city name, and identifying codes are presumably shared with authorities, effectively providing constant surveillance of all users.[16] China's approach to contact tracing presents the most aggressive government control relative to individual liberties of any contact tracing program. While the invasive nature of this app has deterred widespread adoption elsewhere, some of its features are now emerging in apps that are being deployed in other countries.

For example, Singapore's TraceTogether app technically is voluntary, and does not gather exact user location data, but it nevertheless represents one of the more comprehensive monitoring systems adopted.[17] The app uses a cell phone's Bluetooth function to detect and log instances of close contact between persons, stores it on the phone, and then shares that information with the Ministry of Health if a user tests positive.[18] Public health authorities are able to use that data to trace the disease's route of infection and to notify individuals who have come into close contact with a COVID-19 positive person for a period of 30 minutes or longer.[19]

Singapore's app became the model for Australia's COVIDSafe. The app is voluntary, although it appears to have been widely adopted with over 4 million downloads in its first week, and allows the government to warn individuals that they have been exposed to someone who has tested positive.[20] The Australian model will not provide the exposed individual with information on who may have infected them.[21] Despite its widespread acceptance, several limitations were discovered soon after launching, specifically that the app failed to properly log all encounters on "locked" phones where the app was not running in the background.[22]

Israel, similar to South Korea, deployed what is essentially a mandatory tracking program. The Health Ministry supplies the name, ID Number, and cell phone number of those infected with COVID-19 to Shin Bet, Israel's Security Agency, which is then cross-referenced with the Tool, a classified security database that collects cellular data from anyone using telecom in Israel. Those individuals coming into close contact with the infected person receive a text message informing them to quarantine and register with the Health Ministry's database.[23]

The mandatory nature of the tracking, as well as disclosure of the Tool (which pre-dated the pandemic), has produced highly vocal disagreement over the perceived invasion of the privacy rights of Israelis.[24] Criticism resulted in the temporary halt of the surveillance program and development of a voluntary app that initially relied on decentralized GPS for contact tracing, but was recently updated to use Bluetooth to address some of the errors discovered in the first iteration. Despite concerns regarding the sweeping Shin Bet program, it has been reintroduced as the government insisted it is the only way to stay on top of the virus.[25]

The EU Experience

European countries have uniformly rejected mandatory technological tracing. The European Commission has recommended a common EU approach toward contact-tracing apps, but in the absence of an EU-wide mandate, significant differences in approach have emerged.[26] Countries such as Ireland, Germany, Italy, Austria, and Switzerland have opted to use an application programming interface (API) developed jointly by Apple and Google.[27] The Apple-Google API puts a high premium on privacy. The software allows public health authorities to develop mobile contact-tracing apps that utilize their technology.[28] The API uses Bluetooth,[29] there is no centralized storage of data, and the governments are not able to perform basic statistical analysis into a person's contacts or characteristics, which obviously limits the efficacy of tracing in favor of the interests of greater privacy protections.[30]

Other EU-member states, notably France, decided to strike a different balance by forgoing the off-the-shelf convenience of the Apple-Google API, instead investing in their own contact-tracing app that allows for centralized data control. The French junior minister for digital affairs has taken the position that the country's health care crisis response should not be constrained by the privacy policies of Silicon Valley tech giants.[31] By allowing health care professionals to access more precise but intrusive data, in theory France should be able to tackle the virus more effectively, thereby arguably justifying the potential compromise of individual privacy in favor of public health benefits. Supporters of this approach suggest that it will provide researchers with additional data to analyze the spread of COVID-19. [32]

As France forged ahead with its own unique COVID-19 tracking app, however, initial reports suggested that it was not performing as hoped. Despite nearly 2 million downloads, the process had only alerted 14 individuals of possible exposure, even though 68 people informed the app of their infection.[33]

The UK, which had planned to roll out a similar centralized data tracing app, has scrapped that plan for now.[34] Instead, England recently announced trials of its new app, which uses Apple-Google API-based technology. The app uses Bluetooth to identify potential high-risk exposures to infection and will alert people when they have had contact with a person diagnosed with COVID-19. Additionally, it will ask users to scan QR codes at particular locations, so that they can receive alerts if they visited a site with multiple infections.[35] Using the QR codes in addition to the Bluetooth function may address some of the accuracy concerns of Bluetooth effectiveness in highly trafficked locations, like a concert or bar.

The U.S. Experience: State-by-State Experiments

Because the perception and response to COVID-19 has been highly politicized in the United States, and perhaps cautioned by the challenges experienced by other countries, the United States has not adopted a unified approach to contact tracing, and the individual states have been slow to adopt contact-tracing apps. A small number of states have launched voluntary contact-tracing apps that rely on GPS stamps to record the location of COVID-19 positive persons, without—in theory—actually tracking a specifically identified individual.[36]

In April 2020, the state of North Dakota launched an app known as CARE 19 Diary that works with the user to log locations. The app was developed through a partnership with North Dakota and ProudCrowd, a local tech company. Users receive random ID numbers, and locations they visit for longer than 10 minutes are automatically saved throughout the day. If users test positive, they may grant the app permission to share the data with the Health Department for contact tracing and to track the progression of the disease in communities.[37] Neighboring South Dakota will also use the CARE 19 Diary application.[38]

Wyoming has also collaborated with ProudCrowd to bring the application to that state, noting that the more individuals who voluntarily participate, the more effective it will be for contact tracing.[39] The efficacy of these apps has not been validated, and anecdotal evidence based on app reviews suggests that the tracking is inaccurate.[40]

Rhode Island's response app combines the location diary application found in North Dakota's app with a symptom diary. The location diary application tracks the places visited over the last 20 days. The symptom tracker also allows the user to log potential symptoms. The users provide their zip code, which allows the health department to track the spread. Ideally, the individual uses the survey on a daily basis, providing the health department with the most useful data. All individual data from the location diary and the symptom tracker is stored locally on the user's phone and is only shared on a voluntary basis. [41] Rhode Island's app, Crush COVID-19 RI, had a greater number of downloads than any of the other states—though the rate of downloads is still sufficiently modest to call into question its efficacy as a public health protection.[42]

Utah's Healthy Together App allows users to assess their symptoms, find nearby test sites, get instructions for care, and find the hot spots in their state.[43] At its launch, the app used both Bluetooth and GPS to track the location and movement of individuals with COVID-19 in an effort to help public health officials with contact tracing. Because the location tracking function was found to be unpopular, it was turned off (although users may opt-in), which essentially limits the app's effectiveness to that of a personal health tool.[44]

Texas launched a similar program, Texas Health Trace, which allows for a person who tested positive, has symptoms, or thinks he or she has been exposed, to register and receive information and support. Using this system, the Health Department is also able to call the individual to initiate traditional contact tracing.[45] In August, a group of

Texan citizens filed a lawsuit claiming that contact tracing is unconstitutional.[46] While the complaint alleges that the government is tracking Texans involuntarily using their cell phones, the government website indicates that contact tracing is voluntary and provides no indication that movement is tracked or recorded.[47] How this lawsuit develops may significantly inform other states in whether, and if so how, they introduce contact tracing technologies.

Several states have now developed new or supplemental apps based on the Apple-Google API, including Alabama, Nevada, Virginia, Wyoming, North Dakota, New York, New Jersey, Pennsylvania, Delaware, and the territory of Guam. Several others plan to develop an app, including Colorado, Connecticut, Maryland, Oregon, Washington, and the District of Columbia. [48] As discussed above, this technology uses a decentralized identifier system that assigns keys on the user's device. The public health agencies that utilize the app can determine which factors require notification of potential exposure to COVID-19.[49]

On August 5, 2020, Virginia became the first state to launch an app using the API technology. Virginia's app, Covidwise, is voluntary, free, and does not collect personal information or track its user's locations.[50] The app is too new to determine how widely used it will be or its overall efficacy, but the health department has already noted that the app will not work effectively outside the state since there is no federal or interstate coordination.[51]

Conversely, many states have not developed any type of contact-tracing app. South Carolina, for instance, originally intended to utilize the Google-Apple API but lawmakers banned the use of digital contact-tracing apps in a spending bill. Lawmakers expressed privacy concerns that the technology could track users as one of the reasons for the ban.[52] These states continue to use traditional contact tracing which has been known to present numerous challenges, including duplication of efforts by local and state agencies, privacy concerns, and lack of sufficient resources.[53]

Other Examples of Contact Tracing: Higher Education

The challenges associated with contact tracing are not limited to public health agencies, and, in many situations, forgoing digital contact tracing is not an option. For example, as society struggles to return to something closer to normal, workplaces and schools in particular will be pressured to track infected individuals and their movement in more controlled and concentrated environments. Both the University of Arizona and the University of Alabama have stated they intend to implement contact-tracing apps.[54] The University of Alabama's return-to-school plan would require employees and students to log their symptoms.[55] The University has implemented GuideSafe, which incorporates a health check, exposure notification, and an event passport.[56] The exposure notification uses the Apple-Google API to log close contacts and report potential exposure to the user.[57] The app protects user information by using encrypted identification numbers and it does not access GPS location or other data from the user's phone.[58]

Interestingly, COVID-19's transmission is not the first time schools have embraced technology to monitor students on campus. In 2019, the University of Missouri rolled out an optional app to track student attendance.[59] The app uses the school's Wi-Fi and phone sensors to check students into class and ensures that they are present.[60] However, since it does not use GPS, it will not track the students outside of class.[61] The app is also being used by Syracuse and Virginia Commonwealth University.[62]

The potentially "slippery slope" of digitally monitoring university students' class attendance, however, could also become an uncontrolled social experiment, as schools continue to expand the use of these technologies, their functionality becomes more comprehensive, and the assessment of their efficacy continues to be ad hoc. For example, the University of California-Irvine has developed a Wi-Fi-based system that it will use to track an infected person's movements across campus.[63] One tool will be able to monitor how well students are social distancing using anonymized Wi-Fi connectivity datasets that can determine whether spaces are at or over occupancy. It will also employ a tool to monitor traffic flow that enables users to avoid crowded spaces and aid in sanitization efforts. The hot spot function will actually notify people when they have encountered an individual who has tested positive for COVID-19. UC-Irvine represents that each of these applications has built in privacy controls and suggests that they could be easily adaptable for other institutions of higher learning.[64]

Other institutions are applying a technology that utilizes facial recognition technology to identify students. Molloy College has stated their intention to use infrared kiosks in the lobby of its buildings to measure whether students have a temperature greater than 100.4 degrees. This technology will be matched with a catalogue of photographs taken for student IDs.[65]

The use of technological apps to safely return to school is not limited to higher education. Primary and secondary schools in Ohio, Pennsylvania, Massachusetts, and Tennessee have investigated the use of Bluetooth and Wi-Fi based systems to track movement, congregation, and social distancing.[66] The Kiski School, a boarding school in Pennsylvania, is considering another unique solution—implementing a system that would track movement using smart ID cards and Bluetooth technology.[67] While relying on cross-referencing data sets presents a greater risk of generating data that can be used to identify the individual, such systems unmistakably focus on addressing the COVID threat, with potentially unintended consequences to privacy interests.

Challenges Posed by Well-Intentioned Experiments

While the use of contact tracing technology in higher education will provide an interesting series of data sets by which

to judge what are essentially one-off social experiments, a word of caution may be appropriate. Questions remain as to whether the data being gathered is commensurate with the interest being served, as well as the degree to which student participation is in fact "voluntary." Questions as to how that data might be used for other purposes, or the risks posed by unauthorized access to or release of the data, will likely be addressed ad hoc as these apps are used more extensively. Likewise, in the rush to restart, the balance between data collection to combat the spread of COVID on the one hand, and meaningful and informed consent on the other, has not been carefully considered. While downloading an app may be voluntary, it is difficult to get to class without passing through infrared terminals or Bluetooth badges.

The concerns become even more challenging when the data includes sensitive health information. Overlaying temperature checks with student IDs and Bluetooth trackers could easily compromise the anonymity of a "decentralized" app. Given the relatively confined nature of the educational setting, its theoretical privacy protections may be compromised as individuals can likely trace an infection back to a particular class, building, or dormitory. A phone app with a pop-up alert may mean that you were exposed on a bus, elevator, or any random public space, whereas in higher education it will be more difficult to protect identities.

COVID, Privacy, and Antitrust: An Unprecedented Opportunity for Collaboration or a Dangerous Precedent?

Health experts agree that combating COVID-19 will require a great deal of cooperation between the private and public sectors to track and contain the spread of the virus. Some of the tech giants, notably Google and Apple, have leapt into the breach with impressive capabilities and resources that public sector resources simply cannot match, and which hold the promise of making a real difference in combatting the spread of this disease.[68]

The Apple-Google partnership on the API presents an unprecedented breakthrough for the previously siloed technology of Android and IOS devices. The interoperability now available between the two operating systems allows nearly all smartphone users to exchange the Bluetooth "handshakes" necessary for contact tracing.[69] The apps that use this technology will need to adhere to specific privacy controls, which effectively precludes any centralized apps from accessing the extraordinary collective reach of these combined technologies.[70] The Apple-Google partnership, otherwise unimaginable from an antitrust perspective, makes it possible to change the trajectory of the war against COVID by combining their market penetrations with easily normalized applications on their devices.

Organizations with unprecedented market power can collaborate to offer solutions well beyond the reach of public health organizations, but that can present other challenges. It may be unrealistic to expect these collaborating tech giants to subjugate completely their business interests and stop short of using the access and information obtained by their combined monopoly power[71] for other, less public-minded purposes.

The combined reach and technological savvy of the two operating systems opens up other new technological approaches to contact tracing. For example, several European nations initially sought to create a mobile app operable across borders.[72] One approach, the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) would offer technology and services that integrate European privacy standards into a centralized approach.[73] Similar to the API technology, it could be adopted by different apps. Like the Apple-Google function, the PEPP-PT approach would use cell phone data to assess whether an individual had come into close proximity with an infected person.

Germany initially planned to utilize the PEPP-PT, but eventually abandoned this approach when Apple, citing privacy concerns, refused to unlock its operating system to allow for central processing of Bluetooth data.[74] Given Apple's long-standing position on protecting the privacy interests of its users,[75] its decision not to cooperate with Germany does not seem to have been motived by a desire to force Germany to adopt Apple's API rather than develop one of its own. However, without Apple's cooperation, Germany was unable to proceed with the technology. The centralized approach in theory could move forward, but it would be inaccessible to half the mobile market share.

A collaborative effort between two major competitors itself does not raise antitrust concerns per se, but it does invite greater scrutiny. In this case, the two largest market players are allowing interoperability to aid in the efficacy of public health apps during a global pandemic. While pragmatic and even laudatory under the circumstances, the use of their technology is not without its benefits to these dominant players. Whether intended or not, it may have the effect of incentivizing the use of apps compatible with their systems over apps that are incompatible, thus making their current market dominance all the more entrenched. Germany's decision to abandon their own PEPP-PT is a case in point.

There is also the undeniable concern that Apple or Google may find ways to use the information that conceivably could be obtained for their own commercial purposes, even if the privacy of the individuals is not compromised. This data presents a once in a lifetime peek into consumer behaviors and patterns. Google's history of covertly finding ways to mine and use data is well known, and hardly inspires public confidence.[76] For its part, Apple historically has been clear to disavow any such uses, and given the linkage of its brand with privacy protection, Apple may have sufficient consumer credibility for the public to buy into an effective digital contact tracking program.[77]

Those theoretical concerns aside, however, it bears repeating that on its face, the Apple-Google API Exposure

technology incorporates privacy preservation features that make it a much superior option from the perspective of protecting individual liberties as compared to some of the centralized options that store individual data (the full extent of which remains uncertain) on central servers readily accessible to the government. The Apple and Google technology requires the user to *opt-in* to its use, assigns random identifiers that are not tied to an individual, and uses random Bluetooth trackers to limit tracking. The devices will send out a beacon via Bluetooth to other phones, and once a day they will be cross-referenced against beacons for confirmed COVID-19 cases.[78] Those users with possible COVID-19 exposure would be notified by the app with information on next steps from the public health agency managing the regional COVID-19 response.[79] All data will be stored on the device, and the technology is designed so that, at least in theory, none of it is shared with either Google or Apple.[80] This should alleviate the concerns that Google or Apple will make any other use of the data: an entity cannot misuse data it does not have. Given the lack of transparency "behind the curtain" for both Apple and Google, however, privacy advocates are likely to remain skeptical.

Further, the proposed second phase of the technology, which will build the Bluetooth-based contact tracing platform into the underlying platform, has the potential to exacerbate privacy concerns.[81] Apple notes that this stage will require special attention to "privacy, transparency, and consent," as it is unclear how that data will be shared amongst apps and public health authorities, or even within the device's operating ecosystem itself.[82]

In theory, with the API Bluetooth app the only time information is transmitted from the user's phone is when there is a hit on potential exposure or when an individual voluntarily enters their COVID-19 status.[83] But the technological limitations require constant vigilance. By way of example, certain health and fitness apps previously available to iPhone users sent users' personal information to Facebook regardless of the privacy settings selected by the users. While Apple indicated that these apps would need to be modified to remain available to its users,[84] the potential for data collection creep, unintended or otherwise, can never be completely eliminated, even with the Apple-Google partnership. Although the technology is limited only to health authority apps, those are designed by third-party private app developers who may not be completely transparent in the functionality they install. And in contrast to more benign tracking of exercise data, or even consumer activity, the data now potentially at risk represents sensitive health information, and the collateral information that might be generated in connection with this core data may have untold value, and corresponding risk of compromise.

The fact that there have been other instances where the app developers shared data but failed to notify the users does not inspire confidence. For example, ProudCrowd indicated in its privacy settings that the location data would be private and stored only on their servers.[85] Nevertheless, it was later discovered that, depending on certain user settings, the app was sending location and other data to third-parties in violation of its own privacy policy. Instead of stopping this practice, ProudCrowd simply updated its privacy policy to disclose the sharing.[86] Because public confidence in the integrity of any digital tracking system is crucial for voluntary participation, app developers will have to more clearly state their privacy policies and adhere to them.

What's Next?

These contact tracing solutions unquestionably are well-intentioned, but they all have limitations that could compromise privacy or individual liberties. In addition, once these technologies are adopted, when is it appropriate to stop using them? The probability that COVID-19 will one day just disappear seems unlikely. Will the threat of recurrence sometime in the future of a virus that has thus far largely confounded science justify the use of contact tracing for an extended period of time? As these undeniably intrusive technologies become more commonplace, will we find ourselves less sensitive to the use of surveillance technologies in the future? The longer and more broadly we use these applications, the more likely it will be for an extraordinary event to justify mining the data for purposes we cannot anticipate at present.

To ensure that individual liberties are protected, each contact-tracing app should conspicuously disclose how it is being used, the data it collects, the voluntary (or not) nature of its functionalities, and a very clear subset of clauses identifying when it will stop being used and what happens to the data collected once it is shut down. The use of vague language or imprecise concepts—a practice now ubiquitous in virtually all privacy policies—must be avoided. Privacy watchdogs have an equally important role to play, along with the app developer and healthcare authorities, to make these disclosures and protections meaningful. Beyond ensuring that contact-tracing apps are in fact deployed and functioning to protect public health, perhaps the single biggest challenge of achieving that protection will be developing a process that will appropriately protect privacy and personal liberties. ■

[1] *See* Center for Disease Control, *Contact Tracing—CDC's Role and Approach*, https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/contact-tracing-CDC-role-and-approach.pdf (last accessed Oct. 2, 2020); *see also* Michael Fraser et al., *A Coordinated, National Approach to Scaling Public Health Capacity for Contact Tracing and Disease Investigation*, Ass'n of State and Territorial Health Officials, https://www.astho.org/COVID-19/A-National-Approach-for-Contact-Tracing/ (last accessed Oct. 2, 2020).

[2] Bluetooth.com, *The Story Behind How Bluetooth Got Its Name*, https://www.bluetooth.com/about-us/bluetooth-origin/.

[3] Sam Biddle, *The Inventors of Bluetooth Say There Could Be Problems Using Their Tech for Coronavirus Contact Tracing*, Intercept (May 5, 2020), https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/.

[4] Christine Julien, *Contact-Tracing Apps for COVID-19: What You Need to Know (and Do)*, Yahoo News (May 19, 2020), https://www.msn.com/en-us/news

/technology/contact-tracing-apps-for-covid-19-what-you-need-to-know-and-do/ar-BB14ieiA.

[5] Kelly Servick, *COVID-19 Contact Tracing Apps Are Coming to a Phone Near You. How Will We Know Whether They Work*, Science (May 21, 2020), https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how.

[6] *Id*.

[7] Biddle, *supra* note 3.

[8] GPS.gov, *The Global Positioning System*, GPS Overview, https://www.gps.gov/systems/gps/ (GPS combines positioning, navigation, and timing services).

[9] Servick, *supra* note 5

[10] Justin McCurry, *Test, Trace, Contain: How South Korea Flattened Its Coronavirus Curve,* The Guardian (Apr. 22, 2020), https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve; Salvatore Babones, *Countries Rolling Out Coronavirus Tracking Apps Show Why They Can't Work*, Foreign Pol'y (May 12, 2020), https://foreignpolicy.com/2020/05/12/coronavirus-tracking-tracing-apps-cant-work-south-korea-singapore-australia/; Sarah Wray, *South Korea To Step Up Online Coronavirus Tracking,* Smart Cities World (Mar. 20, 2020), https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109.

[11] Ivan Watson et al., *Coronavirus Mobile Apps Are Surging in Popularity in South Korea*, CNN (Feb. 28, 2020), https://www.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html?utm_source=fbCNN&utm_medium=social&utm_term=link&utm_content=2020-02-28T15%3A28%3A07&fbclid=IwAR2y3_c-QdLintfeBR-VNpk0_Ycg1Yc-YdjJeQNDogDjDW14iI8Ah73mtHw.

[12] Wray, *supra* note 10.

[13] Max Fisher, *How South Korea Flattened the Curve*, N.Y. Times (Mar. 23, 2020), https://www.nytimes.com/2020/03/23/world/asia/coronavirus-south-korea-flatten-curve.html.

[14] *Coronavirus: South Korea Confirms Second Wave of Infections*, BBC (June 22, 2020), https://www.bbc.com/news/world-asia-53135626.

[15] Sophia Ankel, *As China Lifts Its Coronavirus Lockdowns, Authorities Are Using Color-Coded Health System To Dictate Where Citizens Can Go. Here's How It Works*, Bus. Insider (Apr. 7, 2020), https://www.businessinsider.com/coronavirus-china-health-software-color-coded-how-it-works-2020-4.

[16] Paul Mozur et al., *In Coronavirus Fight, China Gives Citizens A Color Code, with Red Flags,* N.Y. Times (Mar. 1, 2020), https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

[17] Babones, *supra* note 10.

[18] Team TraceTogether, *How Does TraceTogether Work?,* https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473-How-does-TraceTogether-work (last accessed Oct. 11, 2020).

[19] Babones, *supra* note 10.

[20] *Id*.

[21] *COVIDSafe app*, Australian Government Department of Health, https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#about-the-app (last accessed on Sept. 17, 2020).

[22] Ariel Bogle, *COVIDSafe App Tests Revealed iPhone Performance Issues at Launch that Weren't Shared with the Public,* ABC News (June 16, 2020), https://www.abc.net.au/news/science/2020-06-17/covidsafe-contact-tracing-app-test-documents-rated-poor-iphone/12359250.

[23] Tehilla Schwartz Altshuler et al, *How Israel's COVID-19 Mass Surveillance Operation Works*, Brookings Inst. (July 6, 2020), https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/.

[24] *Id.*; Sam Sokol et al., *Health Ministry Launches Revamped COVID-19 Tracking App*, Times of Isr. (July 27, 2020), https://www.timesofisrael.com/health-ministry-launches-revamped-covid-19-tracking-app/.

[25] Sokol et al., *supra* note 24.

[26] *Covid-19 Tracing Apps: Ensuing Privacy and Data Protection,* Eur. Parliament News (July 27, 2020), https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/COVID-19-19-tracing-apps-ensuring-privacy-and-data-protection.

[27] Ryan Browne, *Europe Starts Rolling Out Coronavirus Contact-Tracing Apps as UK Plans Remain Unclear*, CNBC (June 15, 2020), https://www.cnbc.com/2020/06/15/coronavirus-germany-to-launch-contact-tracing-app-uk-plans-unclear.html; Jason Horowitz et al., *Europe Rolls Out Contact Tracing Apps, with Hope and Trepidation*, N.Y. Times (June 16, 2020), https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html.

[28] Reed Albergotti, *Apple and Google Launch Coronavirus Exposure Software*, Wash. Post (May 20, 2020), https://www.washingtonpost.com/technology/2020/05/20/apple-google-api-launch/.

[29] *Id*.

[30] Horowitz et al., *supra* note 27.

[31] *Id*.

[32] Leo Kelion, *Coronavirus: France's Virus-Tracing App 'Off to a Good Start',* BBC (June 03, 2020), https://www.bbc.com/news/technology-52905448.

[33] David Roe, *France's Covid-19 Tracking App Has Only Identified 14 People at Risk,* RFI (June 24, 2020), https://www.rfi.fr/en/science-and-technology/20200624-france-s-covid-19-tracking-app-has-only-identified-14-people-at-risk.

[34] *See* Rory Cellan-Jones et al., *Coronavirus: The Great Contact-Tracing Apps Mystery*, BBC (July 21, 2020), https://www.bbc.com/news/technology-53485569.

[35] Leo Kelion, *Coronavirus: England's Contact-Tracing App Gets Green Light for Trial,* BBC (Aug. 12, 2020), https://www.bbc.com/news/technology-53753678.

[36] Chas Kissick et al., *What Ever Happened to Digital Contact Tracing?* Lawfare (July 21, 2020), https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing; Benjamin Freed, *Privacy Concerns Have States Taking It Slow on Contact Tracing Apps*, State Scoop (July 17, 2020), https://statescoop.com/contact-tracing-apps-states-privacy/.

[37] North Dakota State Gov't, *Care19*, COVID-19 Resources, https://ndresponse.gov/covid-19-resources/care19 (last accessed on Sept. 16, 2020).

[38] South Dakota State Gov't, *Care19 Diary App*, FAQs About the Care19 Diary App, https://covid.sd.gov/care19app.aspx (last accessed on Sept. 17, 2020).

[39] Tom Coulter, *Governor Announces COVID-19 Contact Tracing Now Available to Wyoming Residents,* Wyoming Trib. Eagle (July 1, 2020), https://www.wyomingnews.com/coronavirus/governor-announces-covid-19-contact-tracing-app-now-available-to-wyoming-residents/article_d9eb6255-603a-5533-955d-24891743b47f.html.

[40] *See* App Store, *Care19 Diary,* Ratings and Reviews, https://apps.apple.com/us/app/care19/id1506077328#see-all/reviews (last accessed Sept. 17, 2020).

[41] Rhode Island Dep't of Health, *Crush COVID RI*, COVID-19 Home, https://health.ri.gov/covid/crush/ (last accessed Sept. 16, 2020).

[42] *See* Kissick et al., *supra* note 36.

[43] *Healthy Together App*, Utah State Government, https://coronavirus.utah.gov/healthy-together-app/ (last accessed Sept. 17, 2020).

[44] Bethany Rodgers, *Utah's Expensive Coronavirus App Won't Track People's Movements Anymore, Its Key Feature,* Salt Lake Trib. (July 11, 2020), https://www.sltrib.com/news/politics/2020/07/11/states-m-healthy-together/.

[45] Texas Dep't of State Health Serv., *Contact Tracing,* COVID-19 Home, https://www.dshs.state.tx.us/coronavirus/tracing.aspx (last accessed 9/16/2020).

[46] *See* Hotze v. Abbot, No. 20-cv-00345 (E.D. Tex. Aug. 11, 2020).

[47] Texas Dep't of State Health Serv., *supra* note 45; Katherine Webster, *Texas Coronavirus Contact Tracing*, Top Class Actions (Aug. 13, 2020), https://topclassactions.com/coronavirus-covid-19/texas-coronavirus-contact-tracing-is-illegal-lawsuit-says/.

[48] Sara Morrison, *Americans Are One Step Closer to a National Contact Tracing App for Covid-19*, Vox (Oct. 2, 2020), https://www.vox.com/recode/2020/10/2/21497729/covid-coronavirus-contact-tracing-app-apple-google-exposure-notification.

[49] Darrell Etherington, *Apple and Google Launch Exposure Notification API, Enabling Public Health Authorities To Release Apps,* Tech Crunch (May 20, 2020), https://techcrunch.com/2020/05/20/apple-and-google-launch-exposure-notification-api-enabling-public-health-authorities-to-release-apps/.

[50] Matt O'Brien et al., *Virginia First To Roll Out Pandemic App from Apple, Google*, AP News (Aug. 5, 2020), https://apnews.com/46b54442d8faf71dab0a5c97b87374d7.

[51] *Id*.

[52] Gregory Barber et al., *Why Contact-Tracing Apps Haven't Slowed Covid-19 in the US*, Wired (Sept. 8, 2020), https://www.wired.com/story/why-contact-tracing-apps-not-slowed-covid-us/.

[53] Benjamin Lesser et al., *Special Report: Local Governments 'Overwhelmed' in Race To Trace U.S. COVID Contacts,* Reuters (Aug. 4, 2020), https://www.reuters.com/article/us-health-coronavirus-tracing-specialrep-idUSKCN2501GK.

[54] Cat Zakrzewski, *The Technology 202: Tech To Contain Coronavirus on College Campuses Sparks Fresh Privacy Concerns*, Wash. Post (July 10, 2020).

[55] Dennis Pillion, *COVID-Tracking App Could Be Key to University of Alabama Reopening, Including College Football,* Alabama.com (June 4, 2020), https://www.al.com/news/2020/06/covid-tracking-app-could-be-key-to-university-of-alabama-reopening-including-college-football.html.

[56] GuideSafe, https://www.guidesafe.org (last accessed Sept. 17, 2020).

[57] GuideSafe, *Alabama's Exposure Notification App*, https://www.guidesafe.org/exposure-notification-app/ (last accessed Sept. 17, 2020).

[58] Pillion, *supra* note 55.

[59] Mara Rose Williams et al., *Invasive or Helpful, MU Using Students' Phones To Track If They Are in Class or Not,* Kansas City Star (Jan. 21, 2020), https://www.kansascity.com/article239139523.html.

[60] *Id*.

[61] Christian Basi, *Attendance App Is Optional for Students Participating in Pilot Project,* Univ. of Miss. Mizzou News (Jan. 27, 2020), https://news.missouri.edu/2020/attendance-app-is-optional-for-students-participating-in-pilot-project/.

[62] Williams et al., *supra* note 58; Drew Harwell, *Colleges Are Turning Students' Phones into Surveillance Machines, Tracking the Locations of Hundreds of Thousands*, Wash. Post (Dec. 24, 2019), https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/.

[63] Zakrzewski, *supra* note 54.

[64] University of California-Irvine, *UCI Researchers Use Campus as Test Bed for Coronavirus Contact Tracing System*, UCI News (July 8, 2020), https://news.uci.edu/2020/07/08/uci-researchers-use-campus-as-test-bed-for-coronavirus-contact-tracing-system/.

[65] Zakrzewski, *supra* note 54.

[66] Will Knight, *Schools Turn to Surveillance Tech To Prevent Covid-19 Spread*, Wired (June 5, 2020), https://www.wired.com/story/schools-surveillance-tech-prevent-covid-19-spread/; Meghan Mangrum, *How a COVID-19 Screening App Can Help Students Return to Chattanooga Christian School's Campus This Fall,* Chattanooga Times Free Press (May 20, 2020), https://www.timesfreepress.com/news/local/story/2020/may/20/how-covid-19-screening-app-help-students-return/523437/.

[67] Knight, *supra* note 66.

[68] *See* Albergotti, *supra* note 28.

[69] Apple, *Apple and Google Partner on COVID-19 Contact Tracing Technology*, Apple Newsroom Update (Apr. 10, 2020), https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/#:~:text=In%20this%20spirit%20of%20collaboration,security%20central%20to%20the%20design.

[70] Apple-Google, *Exposure Notification: Frequently Asked Questions, Preliminary—Subject to Modification and Extension* (Sept. 2020), https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf.

[71] The latest consumer report indicates that Apple iOS has 44% market share and Android has 56%. *See* HT Correspondent, *Apple's iOS Gains Market Share in Q1 but Stays Behind Google's Android: Report*, Hindustan Times: Tech (Apr. 11, 2020), https://tech.hindustantimes.com/tech/news/apple-ios-gains-smartphone-market-share-in-q1-2020-but-stays-behind-google-s-android-cirp-story-kOqz4uxnDO5sqr23d8suAN.html.

[72] Foo Yun Chee, *EU Privacy Watchdog Calls for Pan-European Mobile App for Virus Tracking*, Reuters (Apr. 6, 2020), https://www.reuters.com/article/us-health-coronavirus-tech-privacy/eu-privacy-watchdog-calls-for-pan-european-mobile-app-for-virus-tracking-idUSKBN2101KJ; Leila Abboud et al., *How Europe Splintered over Contact Tracing Apps,* Fin. Times (May 10, 2020), https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10.

[73] Natasha Lomas, *An EU Coalition of Techies Is Backing a 'Privacy-Preserving' Standard for COVID-19 Contacts Tracing*, Tech Crunch (Apr. 1, 2020), https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/.

[74] Tyson Barker, *Germany's Angst Killing Its Coronavirus Tracing App*, Foreign Policy (May 8, 2020), https://foreignpolicy.com/2020/05/08/germany-coronavirus-contact-tracing-pandemic-app/; Douglas Busvine et al., *Germany Flips to Apple-Google Approach on Smartphone Contact Tracing*, Reuters (Apr. 26, 2020), https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J.

[75] Apple, *Privacy Policy*, https://www.apple.com/legal/privacy/en-ww/; *see* Adam Levin, *Why Apple Is Right To Protect Your Privacy*, ABC News (Mar. 8, 2016), https://abcnews.go.com/Business/apple-protect-privacy/story?id=37464507 (last accessed 8/18/2020).

[76] *See* Natasha Singer et al., *Google Is Fined $170 Million for Violating Children's Privacy on YouTube*, N.Y. Times (Sept. 4, 2019), https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html (Google accused of harvesting personal information and using it to profit through targeted ads.)

[77] *See* Jefferson Graham, *Is Apple Really Better About Privacy? Here's What We Found Out*, USA Today (Apr. 17, 2018), https://www.usatoday.com/story/tech/talkingtech/2018/04/17/apple-make-simpler-download-your-privacy-data-year/521786002/; Kate O'Flaherty, *Apple Issues New Blow to Facebook and Google with This Bold Privacy Move,* Forbes (Nov. 6, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/11/06/apple-issues-new-blow-to-facebook-and-google-with-this-privacy-move/#71e6668a481d.

[78] Apple-Google, *supra* note 70.

[79] Google, *Exposure Notifications: Using Technology To Help Public Health Authorities Fight COVID-19,* COVID-19 Information and Resources, https://www.google.com/covid19/exposurenotifications/ (last accessed on 8/13/2020).

[80] Apple-Google, *supra* note 70.

[81] Apple, *supra* note 69.

[82] *Id*.

[83] Apple-Google, *supra* note 70.

[84] Laura Sydell, *Storing Health Records on Your Phone: Can Apple Live Up to Its Privacy Values?* NPR (Feb. 27, 2019), https://www.npr.org/2019/02/27/697026827/storing-health-records-on-your-phone-can-apple-live-up-to-its-privacy-values.

[85] Stephen Groves, *Tech Privacy Firm Warns Contact Tracing App Violates Policy*, ABC News (May 22, 2020), https://abcnews.go.com/Health/wireStory/tech-privacy-firm-warns-contact-tracing-app-violates-70839803.

[86] Dominic Dhil Panakal, *Dakotas Slip in COVID-19 Contact Tracing Privacy Protection,* Nat'l L. Rev. (June 2, 2020), https://www.natlawreview.com/article/dakotas-slip-covid-19-contact-tracing-privacy-protection.