COVID-19 Rapid Response Impact Initiative | White Paper 22

Digital Tools for COVID-19 Contact Tracing:

Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns

July 2, 2020

Koustubh "K.J." Bagchi[1]
Christine Bannan[2]
Sharon Bradford Franklin[3]
Heather Hurlburt[4]
Lauren Sarkesian[5]
Ross Schulman[6]
Joshua Stager[7]

Abstract

Many state governments and public health authorities in the United States are turning to digital tools to assist contact tracing efforts in response to the coronavirus pandemic despite equity, privacy, and civil liberties concerns. The digital divide, pronounced lack of trust in government among certain communities, and privacy risks posed by collecting personal data at scale make effective deployment of digital contact tracing tools challenging. But if governments decide they need to supplement manual contact tracing due to capacity issues, digital tools that use exclusively Bluetooth-based technology may be useful, as long as public health authorities implement proper safeguards. This paper outlines the equity, privacy, and civil liberties risks posed by digital tools as well as safeguards that policymakers can adopt to mitigate these concerns. Further, the paper recommends that policymakers take affirmative steps to address vulnerable populations that are unlikely to be reached by digital apps, partner with developers and community organizations, promote public education campaigns when deploying digital tools, take steps to close the digital divide, and pass comprehensive privacy legislation with effective enforcement mechanisms.

[1] Senior Policy Counsel, New America's Open Technology Institute
[2] Policy Counsel, New America's Open Technology Institute
[3] Policy Director, New America's Open Technology Institute
[4] Director, New Models of Policy Change, New America's Political Reform Program
[5] Senior Policy Counsel, New America's Open Technology Institute
[6] Senior Counsel & Senior Policy Technologist, New America's Open Technology Institute
[7] Senior Policy Counsel, New America's Open Technology Institute

Table of Contents

01 Introduction

As states, counties, and foreign governments move to reopen society amid the ongoing coronavirus pandemic, most are relying upon models that center around testing and extensive contact tracing. The Safra Center's "Roadmap to Pandemic Resilience,"[8] released in April 2020, sets out a comprehensive approach to enabling society to reopen, based on testing, tracing, and supported isolation (TTSI). The contact tracing envisioned in the Roadmap involves a robust combination of traditional manual approaches and reliance on digital tools. Likewise, as state governments are now planning and implementing their reopenings, many are considering combined approaches that supplement manual tracing with digital tools. A number of Asian and European countries have also instituted such mixed systems in recent months.

A variety of policy experts, technology companies, and public health officials have argued that digital tools may be able to expand the reach of traditional manual contact tracing systems and provide a rapid alert system that enables potentially exposed individuals to seek testing.[9] While, as this paper describes, it is not clear that such tools can be effective given the scale and rapid spread of the coronavirus pandemic, we should consider how they might play a role in the United States' pandemic response. This white paper aims to examine the equity, privacy, and civil liberties concerns raised by digital contact tracing tools, to outline safeguards that promise to mitigate these concerns, and where possible, to explain how to incorporate these safeguards.

We recognize that traditional manual contact tracing techniques also present equity, privacy, and civil liberties issues. Traditional contact tracing requires the collection of personal medical and behavioral

[8] Allen et al., "Roadmap to Pandemic Resilience: Massive Scale Testing, Tracing, and Supported Isolation (TTSI) as the Path to Pandemic Resilience for a Free Society."
[9] Simpson and Conner. "Digital Contact Tracing To Contain the Coronavirus"; Kahn and Johns Hopkins, *Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance*.

information from infected individuals, and just as with digital data, this collected information is subject to risks of misuse and oversharing. For example, the Cook County Board of Commissioners passed a resolution—later vetoed by the Board's president—that would have required the personal information of those who tested positive for COVID-19 be disclosed to law enforcement.[10] Such a requirement would have severe implications for equity, privacy, and civil liberties.

However, an extended discussion of the risks associated with manual contact tracing techniques is beyond the scope of this paper. This paper focuses on the issues presented by digital tools because they create novel and additional risks relative to traditional manual contact tracing. First, digital tools collect an exponentially greater volume of data, including data on vast numbers of individuals who are not infected and have not even been in contact with infected individuals. Manual contact tracing, by contrast, is limited to infected individuals and their contacts. Second, because public health agencies generally lack in-house technical expertise and capacity, digital tools are designed and operated by private companies in partnership with public health authorities, rather than by public health authorities directly. This creates questions about corporate access to data that do not arise in manual contact tracing. Third, the risk of data breach is much more significant: an attack could expose the data of millions of individuals. And finally, while law enforcement access is also a risk in manual systems, the volume and types of data collected by digital tools make these systems more attractive to law enforcement and more vulnerable to mission creep.

Before seeking to outline a rights-protective approach to using digital tools for contact tracing, we must set forth some key principles that frame our analysis. First, when policymakers use big data solutions as part of pandemic response, they should follow the guidance of public health experts to determine

[10] Yin, "Cook County Board President Toni Preckwinkle Vetoes 'Extraordinarily Bad' Plan to Share Coronavirus-Positive Addresses with First Responders."

[11] Amnesty International USA, "Contact Tracing App Exposed Sensitive Personal Details of over One Million."

what is necessary and efficacious in combating the virus. Technology is not the solution for every problem, and we must be guided by experts in epidemiology and public health in designing solutions that will work.

Additionally, while effectiveness of contact tracing may come in degrees, three conditions should be met for a large-scale contact tracing system to be most effective. First, very widespread and accessible testing must be available, as laid out in the first pillar of the "Roadmap to Pandemic Resilience." If people cannot easily get tested, tracing will be far from complete. Countries that have had some success with limiting the spread of the coronavirus (albeit with setbacks in the cases of Singapore and South Korea, and with invasive government surveillance approaches in China and South Korea) have first had widespread testing available. There is no model for successful COVID-19 containment that does not include an extensive testing regime. Although some states are making progress in developing testing capacity,[12] it is not clear if or when the necessary level of testing will be available across the United States.[13] Second, the structures to permit supported isolation—the third pillar of the Roadmap—must also be in place, so as not to create disincentives for individuals to either get tested or to participate in contact tracing efforts. These supports include job protection and income compensation, health care and family support, and protection for vulnerable communities reluctant to engage with the authorities. Third, global and U.S. experience suggests that contact tracing regimes are more effective when they are designed and implemented in partnership with vulnerable communities and those most impacted by the virus.

Each of these conditions brings with it important equity concerns that cannot be ignored, especially as our nation wrestles with the consequences of structural racism and inequality across all of public life. For example, protest leaders have issued COVID response demands, highlighting what is needed to allow Black and other marginalized communities to benefit equally from a contact tracing regime:

[12] TestAndTrace, "What U.S. States Are Ready To Test & Trace?"
[13] Osterholm and Olshaker. "Let's Get Real About Coronavirus Tests."

universal paid leave, provision of shelter, food, housing and healthcare for all, decarceration, and limitation of law enforcement powers.[14] Developing and implementing contact tracing tools now requires a process of equity and inclusion very different from how the health tech industry usually operates; established manual tracing best practices will provide some guidance, but the challenge is significant.

[14] Movement for Black Lives, "National Demands for COVID-19."

02 The Components of Contact Tracing

Traditional Contact Tracing Methods and New Challenges

Contact tracing is a traditional public health technique used to combat infectious disease outbreaks. It enables public health officials to identify individuals who have been exposed to someone who has contracted an infectious disease, so that exposed individuals can get tested and can quarantine themselves if needed. Traditionally, contact tracing involves trained public health personnel speaking directly with individuals who have been exposed to and identified by an infected person. Public health officials have long used contact tracing to break chains of transmission of infectious diseases, but the COVID-19 pandemic has posed unprecedented challenges due to its scale and the speed of its transmission worldwide.

Two elements of COVID-19 make contact tracing especially important in this pandemic, but likewise especially challenging: the long incubation period and the frequency of asymptomatic transmission. As compared with other viruses, COVID-19 has a relatively long incubation period: the median time from infection to onset of symptoms is five days, but nearly all infected persons who will show symptoms will do so within twelve days.[8] More problematic yet, recent coronavirus data demonstrate that a substantial proportion of transmissions, perhaps as high as 50 percent, occur between individuals who are not symptomatic.[9] Because health experts now believe that asymptomatic spread of COVID-19 is a significant source of infection, health authorities know that they need to work to identify potentially infected people before they show symptoms.

Accordingly, speed is essential for contact tracing, but state, county, and municipal health authorities have only limited personnel available for manual contact tracing. Former director of the Centers for

[15] Lauer et al., "Incubation Period of Coronavirus Disease 2019 (COVID-19) From Publicly Reported Confirmed Cases: Estimation and Application."
[16] Hub Staff, "Asymptomatic Spread Makes COVID-19 Tough to Contain."

Disease Control (CDC) Tom Frieden has reportedly estimated that “[w]e need an army of 300,000 people”[17] to trace the coronavirus in the United States, but as of late April, we only had about 8,000 contact tracers working nationwide.[18] Promisingly, there are new initiatives to train contact tracers, such as ones through Johns Hopkins University, which has established a new online course to train numerous people to work as contact tracers,[19] and UC San Francisco, which is partnering with the California Department of Public Health to provide similar training.[20] Moreover, some states are quickly working to hire manual contact tracers to make up for this shortfall,[21] but states will likely still have difficulty hiring and training contact tracers at the necessary rate.

Contact tracers undergo training to develop the skills needed to deal with the highly sensitive and complex issues associated with infectious disease and human behavior. These skills have been described as “somewhat of an art” that technology may not be able to replicate.[22] The CDC notes that “contact tracing is a specialized skill. To be done effectively, it requires people with the training, supervision, and access to social and medical support for patients and contacts.”[23] The current pandemic is placing these skills under added pressures as public health authorities are not able to conduct these manual approaches with available resources.

For these reasons, during the current coronavirus pandemic, various countries, public health authorities, researchers, and app developers have designed digital tools to assist in contact tracing efforts.

[17] Fox, “We Need an Army’: Hiring of Coronavirus Trackers Is Likely Set to Soar.”

[18] Haskins et al., “We Need An ‘Army’ Of Contact Tracers To Safely Reopen The Country. We Might Get Apps Instead.”

[19] Pearce, “Johns Hopkins Launches Online Course to Train Army of Contact Tracers to Slow Spread of COVID-19.”

[20] Kurtzman, “UCSF Partners with State to Develop Public Health Workforce for COVID-19 Response.”

[21] Nadi, “Inside an ‘Army’ of COVID-19 Contact Tracers in Massachusetts”; and Simmons-Duffin, “States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago.”

[22] Holder, “Who Wants to Be a Contact Tracer?”

[23] CDC, “Coronavirus Disease 2019 (COVID-19).”

The Components of Contact Tracing

Traditional Contact Tracing Methods and New Challenges

Proponents of these digital tools aim to increase the speed and reach of traditional contact tracing methods, which can be slow, labor-intensive, and costly. Italy's minister for technological innovation views the country's app Immuni as a tool with the potential for a "major impact" on public health.[24] The academics at University of Washington helping to develop an exposure notification app known as CovidSafe view these apps as tools that can augment traditional contact tracing but not replace it.[25] An infectious disease specialist at Mayo Clinic who has contributed to the SafePlaces app believes that "contact tracing is a critical intervention" and that digital tools can enhance contact tracing capabilities and help public health officials to intervene expeditiously.[26] Similarly, the dean of UAB School of Medicine and chair of the re-entry task force for the University of Alabama system views the state's app as their "best chance for actually surviving through this without undue damage and havoc, [a]nd having a chance to move into a future where we may eventually get a vaccine."[27]

However, as this paper outlines, there are many open questions regarding the efficacy of such digital tools. Moreover, there is little to no precedent for automating the delicate work of contact tracing. Accordingly, digital tools should be considered as methods to augment, but not replace, traditional manual contact tracing by public health officials.

At this stage, we cannot yet know the relative reach of traditional contact tracing methods and digital tools, or the extent to which digital tools will enable contact tracing to be conducted at scale. Nonetheless, if they are implemented in a rights-protective way, digital tools to support contact tracing have the potential to assist public health authorities in combating this pandemic.

[24] Horowitz and Satariano, "Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation."
[25] McQuate, "Contact-Tracing App That Helps Public Health Agencies and Doesn't Compromise Your Privacy."
[26] MIT Media Lab, "Safe Paths: A Privacy-First Approach to Contact Tracing."
[27] Pillion, "Alabama Balances Privacy against Accuracy in Contact Tracing App."

What Digital Tools May Be Helpful

There are a variety of digital tools under consideration for supporting contact tracing efforts. Some tools may assist contact tracers in managing caseloads[28] and in coordinating outreach to ensure that people with the necessary language skills are assigned where needed. Other digital tools are being proposed and developed with the goal of assisting public health authorities to identify people who may have been exposed to an infected person. These tools have been referred to as "digital contact tracing apps," although more recently, many proponents have adopted the more precise description of "exposure notification apps." Developers are designing such apps to use data generated by smartphones in ways that can expand the reach of manual contact tracing approaches.

In deciding what digital tools, if any, to adopt, health authorities must carefully consider what specific data is useful. Digital tools should not collect individuals' location data through cell site location information (CSLI) or Global Positioning System (GPS) information. These types of data are generated by individual cellphones and collected by phone providers and various apps in connection with the services they offer. Contrary to what some have argued,[29] collecting such location information is neither useful nor appropriate. It is not useful because phone location data is not precise enough to allow assessments of whether particular individuals came close enough for transmission of the virus;[30] and while GPS is more accurate than CSLI, it only works when people are outside, its accuracy can vary depending on a number of factors, and its drastic negative impact on battery life means that uptake will be seriously hampered. Use of CSLI and GPS is not appropriate because collecting such information about specific individuals would be extremely privacy invasive, as it can reveal their paths of travel

[28] Bourdeaux et al., "How Human-Centered Tech Can Beat COVID-19 through Contact Tracing."
[29] Albergotti and Harwell, "Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless."
[30] Landau, "Location Surveillance to Counter COVID-19: Efficacy Is What Matters."

and intimate details about their daily lives.[31] As a result, contact tracing apps should not rely on CSLI or GPS, and governments should not be collecting this data for individuals. However, it may be appropriate for public health authorities to seek such location data in aggregate anonymized form; heat maps and analytical tools that rely upon aggregate location data may provide helpful information for planning pandemic responses.[32]

Contact tracing tools that rely on Bluetooth technology to measure proximity should provide a better proxy for determining exposure to the virus, though their accuracy is uncertain. There are several models for such apps, most of which have been inspired by Singapore's TraceTogether app initiated in March.[33] In May, Apple and Google launched interoperable Application Programming Interfaces (APIs) that will support exposure notification apps as long as they are approved by public health authorities and comply with the Apple/Google privacy requirements.[34] The TCN Coalition, an international coalition of technologists formed in April, has developed and promoted recommendations to incorporate privacy safeguards into the design of such exposure notification tools.

These Bluetooth-enabled apps, once voluntarily downloaded on individuals' smartphones, would cause the phones to send out anonymized signals that other phones in close proximity and also running the app would detect and catalog. Whenever an app user later tests positive for the coronavirus, the user is then able to report the test result, with a certification, to the relevant public health authority. That authority could then denote this in the app so that the app could alert all other phones that had detected a signal from the infected person's phone over the past fourteen days. An app user receiving such an alert would then know to seek testing.

[31] Franklin, "Right and Wrong Ways to Use Location Data in the Pandemic."
[32] See ibid.
[33] Ungku, "Singapore Launches Contact Tracing Mobile App to Track Coronavirus Infections."
[34] Google, "Exposure Notification API Launches to Support Public Health Agencies."

The Components of Contact Tracing

What Digital Tools May Be Helpful

While many questions remain about their operation, these Bluetooth systems are inherently more effective and privacy protective as tools to support contact tracing than the collection of individuals' CSLI or GPS data. Bluetooth technology can measure the much shorter distances necessary for contact tracing, and with Bluetooth apps, the phones are simply measuring their proximity to one another and not the precise location of either phone. There are also several critical components that should be incorporated into the design of such apps to ensure that they are as rights-protective as possible. In particular, the apps must be voluntary, with individuals choosing to download and use them. In addition, implementation must be decentralized, so that there is no central government authority collecting all the emitted Bluetooth signals; rather, the signals generated and detected by each phone should be stored on individual devices. Another critical safeguard is to ensure that the apps generate random, anonymized, and constantly changing signals to avoid any risk that individuals can be reidentified or tracked. Finally, no data from these apps should ever be used commercially.

Some have proposed apps that rely upon Bluetooth proximity data combined with individual location data. However, it is the Bluetooth proximity information, not GPS or CSLI data, that can show whether two individuals have come close enough to one another to create a risk of exposure. Public health authorities should not collect individuals' actual location information even as part of hybrid systems. Location data that shows an individual's actual path of travel can much more easily lead to reidentification and tracking of specific people, and it is unclear that it would provide any improved efficacy. For example, North Dakota has introduced an exposure notification app called Care19 that relies on such a hybrid approach involving Bluetooth and GPS, but it has been riddled with accuracy issues due to both its inconsistent recording of GPS data and the insufficient granularity of the GPS data it does record.[35]

[35] Morse, "North Dakota Launched a Contact-Tracing App. It's Not Going Well."

03 Equity and Effectiveness Issues with Contact Tracing

The greatest challenges for digital exposure notification systems are the intertwined issues associated with equity and effectiveness. First, despite its relative benefits over the use of CSLI or GPS data, the effectiveness of Bluetooth technology to support contact tracing remains unconfirmed—for both reasons related to the technology itself and much larger issues related to adoption of such technology. Further, digital tools, even more so than traditional manual contact tracing approaches, are not equally available to—or trusted by—all communities, and reliance on such tools risks exacerbating inequities already present across the United States. Moreover, to the extent that digital tools are not equally available and widely adopted, this will hinder their effectiveness in assisting public health authorities to conduct contact tracing at scale.

Certain strategies—such as building in privacy safeguards when designing digital tools, combating misinformation, and conducting public education campaigns—can help minimize these obstacles, although real change will likely require long-term efforts and investment. Meanwhile, awareness of these issues can assist public health authorities to design solutions that will be as rights-protective, widely adopted, and effective as possible.

Effectiveness Issues in Bluetooth Technology

Bluetooth signals may lead to both false positives and false reassurances of a lack of exposure. For instance, exposure notification apps can cause false positives because Bluetooth signal strength varies depending on the phone's position and whether a person carries the device in a pocket or a bag.[37]

[36] Sarkesian, "Amid Reopenings, Technology Alone Won't Stop the Coronavirus."
[37] There is also an open question as to whether measuring the strength of a Bluetooth signal gives any information as to the distance between devices at all. Leith and Farrell, "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection."

Bluetooth signals may show connections when individuals are too far apart to transmit the virus (even as far as 30 feet apart) and are separated by walls—these crucial details make all the difference in terms of one's exposure risk, and cause false positives.[38] Individuals living in apartment buildings may therefore be more likely to encounter false-positive notifications, as Bluetooth can ping nearby phones through walls and even floors, meaning that Bluetooth could indicate a possible exposure among neighbors who did not actually breathe the same air.[39]

Conversely, it is also likely that the apps will undercount potential exposures. Even if people widely adopted and used Bluetooth exposure notification apps—which, as discussed below, is far from certain—there will be an undercount of exposures both because Bluetooth technology can be unreliable and because public health officials are constantly learning more about the novel coronavirus and its symptoms.[40] As of March, many believed that fevers were a nearly requisite symptom of coronavirus, but since then evidence has mounted showing that presymptomatic and asymptomatic people could also pass the virus to other individuals. Significantly, Bluetooth applications can merely inform individuals that they have not been around an individual who was diagnosed positive (and who is also using the app), but certainly cannot detect undiagnosed cases. Bluetooth apps could consequently lead to a false sense of security among the public, though the apps can only, at best, inform individuals of recent exposures.

Further, some elements of disease transmission may be challenging for Bluetooth or any technology to trace: because it is an airborne respiratory virus, coronavirus is mostly transmitted when individuals are indoors and the viral load, or amount of virus one carries when infected, is significant. In a study from China of over 7,300 cases, only one case was transmitted outdoors.[41] And while it has not yet been

[38] Newton, "Why Bluetooth Apps Are Bad at Discovering New Cases of COVID-19."
[39] Landau, Lopez, and Moy, "The Importance of Equity in Contact Tracing."
[40] Landau, "Looking Beyond Contact Tracing to Stop the Spread."
[41] Qian et al., "Indoor Transmission of SARS-CoV-2."

definitively proven, a study from China shows that higher exposure doses lead to higher viral loads, which lead to more severe cases of COVID-19.[42] Both of these elements—whether individuals are in proximity outdoors or indoors, and how much of the virus one may have been exposed to—are difficult if not impossible for the current technology to measure. However, as discussed below, the most significant challenges to overcome in order for exposure notification apps to be effective are obstacles that affect how widely the public, in particular the most vulnerable populations, will adopt and use them.

Biggest Hurdles: Public Trust & Equity Issues Which Impact Effectivenes

For a Bluetooth-based contact tracing system to be effective, many epidemiologists estimate that roughly 50 to 70 percent of a population would need to participate for the app to be used to replace rather than supplement manual contact tracing.[43] In order to participate, individuals will need to own a smartphone made in the last five years,[44] download an app, and carry their phone with them at all times, with Bluetooth enabled. However, of the several countries that have created COVID-19 contact tracing apps, the highest adoption rate is in Iceland, where only 38 percent of residents have downloaded the app.[45] Yet some experts, such as an infectious disease specialist at Oxford University's Big Data Institute, estimate that an adoption rate of slightly more than 10 percent of a population could cut down on infections, because one infection could be prevented for every one to two users.[46]

Public Trust

Public trust will play a significant role in promoting robust participation. However, as discussed further

[42] Hogan, "How Much of the Coronavirus Does It Take to Make You Sick?"
[43] Fussell and Knight, "The Apple-Google Contact Tracing Plan Won't Stop Covid Alone."
[44] Bradshaw, "2 Billion Phones Cannot Use Google and Apple Contact-Tracing Tech."
[45] O'Neill et al. "A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them"; Johnson, "Nearly 40% of Icelanders Are Using a Covid App—and It Hasn't Helped Much."
[46] Horowitz and Satariano, "Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation."

below, much of the public lacks such trust both in the government and in big tech companies, and a troubling combination of misinformation around COVID-19 and justified historical grievances have fueled a heightened sense of mistrust. In some communities, public health responses have become identified with partisan politics, while others may experience contract tracing methods as a continuation of histories of heavy policing and surveillance. A lack of public trust can also pose barriers to manual tracing efforts, but these challenges are compounded for digital tools that also require trust in companies. Indeed, the companies involved in the development of contact tracing applications will have to prove their trustworthiness after many years of technology companies disappointing consumers with their poor handling of personal data. The proliferation of various apps purporting to assist with contract tracing, many of which do not incorporate the safeguards recommended in this paper, is compounding this trust problem.

Combatting the misinformation surrounding the many varying app proposals moving forward will be a challenge for governments and app providers alike, and will affect much of the public. Already, misinformation has been having a detrimental effect in the spread of coronavirus, and those with less access to reliable resources are likely to suffer the most.[47] The proliferation of misinformation in the time of COVID-19 has spread harmful claims that appear, in some cases, to have been specifically targeted at marginalized communities.[48] One study indicated that a number of factors play into the spread of the false belief that the coronavirus was created in a lab, including education level, political affiliation, and race.[49] In particular, those with a bachelor's degree or more education were less likely than those with a high school diploma or less education to believe the coronavirus was created in a lab. Addressing the spread of misinformation and properly educating the public regarding coronavirus will be critical to reaching vulnerable communities with any digital tracing tools.

[47] Bursztyn, "Misinformation During a Pandemic."
[48] Ross, "From White Conservatives to Black Liberals, Coronavirus Misinformation Poses Serious Risks."
[49] Schaeffer, "Nearly Three-in-Ten Americans Believe COVID-19 Was Made in a Lab."

Unfortunately, the public health system has a record of discrimination, mistreatment, and inconsistency toward communities of color.[50] For example, in the 1972 Tuskegee Study conducted by the U.S. Public Health Service doctors knowingly failed to treat Black men diagnosed with syphilis, though treatment was readily available at the time.[51] The outrage and mistrust generated by this discriminatory study still impact the Black community to this day.[52] Using health services also leaves some already-vulnerable individuals further exposed, as they risk encountering immigration and law enforcement personnel. In a recent example, a man was arrested by U.S. Immigration and Customs Enforcement (ICE) agents as he left an emergency room,[53] even though hospitals have been considered "sensitive locations" by ICE and should be avoided for immigration enforcement.[54] While ICE has stated that it will modify its enforcement efforts during COVID-19 around "sensitive locations,"[55] the agency's past actions do not raise the public's confidence—and data from across the country shows that anxious immigrants are avoiding testing and treatment for this reason.

In addition to mistrusting government entities, the general public has consistently indicated an overall skepticism of the technology sector in recent years. Prior to the onset of the pandemic, tech companies had developed a negative reputation for gathering users' personal data and selling or transferring that data to third parties without informing users. The most infamous example of this improper secondary use of information is the Facebook and Cambridge Analytica scandal,[56] but there are numerous other examples, including cases involving the misuse of location information. Indeed, earlier this year, the Federal Communications Commission (FCC) fined the nation's four largest wireless carriers for selling

[50] Hardeman et al., "Structural Racism and Supporting Black Lives: The Role of Health Professionals."
[51] CDC, "U.S. Public Health Service Syphilis Study at Tuskegee."
[52] O'Donnell, "Coronavirus: Some Fear Black People Won't Get Vaccine. Here's Why."
[53] Hall, "ICE Criticized for Arrest at Scranton Hospital."
[54] See Morton, Memorandum,"Enforcement Actions at or Focused on Sensitive Locations," Oct. 24, 2011; and Aguilar, Memorandum, "U.S. Customs and Border Protection Enforcement Actions at or Near Certain Community Locations," Jan. 18, 2013.
[55] ICE, "ICE Guidance on COVID-19."
[56] Confessore, "Cambridge Analytica and Facebook:The Scandal and the Fallout So Far."

their customers' location information without the customers' consent.[57] A Pew Research Institute study conducted in June 2019 found that 79 percent of adults surveyed said they were at least somewhat concerned about how companies were using the data collected about them.[58] In addition, that study found that 70 percent of those surveyed felt their personal information was less secure than it was five years ago. The Pew results indicate an overall lack of trust in the access that app developers have to user data, and may imply a reluctance to use digital tools to support contact tracing if those tools require users to share data with a tech company.

This dynamic of mistrust toward tech companies, especially with regard to privacy, has not been alleviated even as tech companies attempt to provide solutions for combating the pandemic. Even though many members of the public have been sacrificing their civil liberties due to the need for ongoing isolation, Americans seem skeptical of digital contact tracing tools—though they vary on whom they trust, with what information, and for what purpose. In a recent *Washington Post* survey, three in five adults surveyed indicated that they would be either unable or unwilling to use the exposure-alert system under development by Apple and Google.[59] And a May Axios survey showed that who is providing the apps is significant: while 51 percent of Americans would participate in apps provided by the CDC or public health officials, only 33 percent would participate if the providers were big tech companies, and even fewer would partake if the federal government were providing them.[60]

A further complication is that Americans are very unclear on who, in fact, is the entity providing these apps. Many apps will be offered on Apple and Google's interfaces, but they will be created by various

[57] FCC, "FCC Proposes over $200 Million in Fines against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data."
[58] Auxier, "How Americans See Digital Privacy Issues amid the COVID-19 Outbreak."
[59] Timberg, Harwell, and Safarpour, "Most Americans Are Not Willing or Able to Use an App Tracking Coronavirus Infections. That's a Problem for Big Tech's Plan to Slow the Pandemic."
[60] Talev, "Americans Highly Resistant to Participating in a Contact Tracing Program."

app developers in conjunction with different state and local governments. With many varying apps being offered—one for each state, if not more—the patchwork of apps with different approaches (some following the Apple/Google API, some collecting location data, and perhaps some in between) will likely confuse Americans' analysis of whether they trust the provider and are willing to participate.

Equity Issues

Any contact tracing tools that rely on smartphones risk exacerbating a wide range of inequities in American society that stem from disparities in income, age, race, language proficiency, and geography, among other factors. Many of these inequities are deep-seated and not easily remedied. Accordingly, relying on digital tools for contact tracing risks focusing our public health response on the most digitally connected, while neglecting precisely the populations that are most at risk for infection.

It is important to note that manual contact tracing also presents equity considerations that can decrease the likelihood of robust participation. Manual contact tracing requires significant investment by public health authorities to hire a multitude of contact tracers and to subsequently supply them with the case management tools necessary to conduct in-depth surveys of affected individuals. The first step in manual contact tracing involves interviewing the infected person to make a list of all the persons with whom they may have come in contact. With this pandemic, due to the contagiousness of the virus and the lack of any vaccine or proven treatment, there has been increased reliance on interviews conducted over the phone. This exacerbates certain obstacles such as outdated contact information, lack of language comprehension, and a mistrust of the contact tracer.[61] However, the personal approach that manual contact tracers provide can be more effective in building trust with marginalized communities than digital approaches.[62]

[61] Greiner et al. "Addressing Contact Tracing Challenges—Critical to Halting Ebola Virus Disease Transmission."
[62] Sellers and Guarino, "Contact Tracing Is 'Best' Tool We Have until There's a Vaccine, Health Experts Say."

In addition, the entire contact tracing enterprise assumes that, once a risk is identified, individuals will self-quarantine and get tested and treated as necessary. Inequitable distribution of access to sick leave, health care, housing, and food will depress participation in every stage of a tracing regime unless jurisdictions plan ahead to put those services in place—and make the most vulnerable communities aware that they exist and are safe to use.[63]

Yet contact tracing through digital tools is subject to additional and heightened equity concerns, particularly given the need for smartphone ownership and digital literacy to participate. While 81 percent of Americans own a smartphone, this means that nearly one-fifth of the population does not.[64] Moreover, it is unclear how many Americans own smartphones that support the technology that contact-tracing apps may require, such as low-power Bluetooth chips, the newest operating systems, and sufficiently robust batteries—but the number is likely well below 81 percent. Moreover, the population without smartphones is largely made up of lower-income communities[65] and seniors[66]—precisely the demographics that are most at risk of COVID-19 infection. Older Americans are also more likely to lack sufficient digital literacy skills.[67] These skills would be critical for maneuvering a digital exposure notification system, which requires familiarity with Bluetooth functionality, engaging with a phone's notification system, and correctly deploying a phone's contact tracing app to alert others of their potential exposure to coronavirus. Further, in the public debates over what role digital tools can play in contact tracing, not enough analysis has been provided on how individuals with lower levels of English proficiency will be able to participate in the system.

To the extent that exposure notification apps may induce people living in proximity to older Americans

[63] The experience of Chelsea, Massachusetts is sobering in this regard. See Barry, "In a Crowded City, Leaders Struggle to Separate the Sick from the Well."
[64] Pew Research Center, "Mobile Fact Sheet."
[65] Anderson and Kumar, "Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption."
[66] Anderson and Perrin. "Technology Use among Seniors."
[67] Fields, "We Are Leaving Older Adults out of the Digital World."

or others who lack smartphones to get tested or self-quarantine, the apps may provide some benefit to individuals who do not themselves participate in the system. However, any smartphone-based application to assist contact tracing will be far less effective in reaching minority and vulnerable communities, thereby having a serious impact on the efficacy of the tool.

For a multitude of reasons, COVID-19 is disproportionately impacting racial and ethnic minority groups, which makes it even more important to develop a system that will not leave these communities behind.[68] As noted, misinformation about the virus has already spread particularly widely among marginalized groups, and it has also been rampant on platforms reaching a variety of demographics across the country. This mistrust between government entities and marginalized communities, as well as lower levels of digital literacy in such communities, must also be accounted for in developing an adoption strategy.

Implementing a system where users are *required* to download an exposure notification app or other digital contact tracing tool in order to access public spaces would exacerbate these equity issues. Policies mandating app usage have been adopted in other countries, and some employers in the United States are considering plans to require exposure notification apps for employees returning to work.[69] If downloading and using an exposure notification app becomes a requirement to determine access to certain spaces, those who do not possess a smartphone or knowledge of how to utilize a contact tracing app would be excluded from basic aspects of everyday life, potentially including their place of employment, schools, and grocery stores. The disparities that already existed pre-pandemic would become compounded as a result.

Digital exposure notification apps also risk leaving behind large swaths of rural America that lack cellular

[68] CDC, "COVID-19 in Racial and Ethnic Minority Groups."

[69] Mozur et al., "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags; Coombs," "Microsoft and UnitedHealth Offer Companies Free App to Screen Employees for Coronavirus";. Leswing, "Companies Could Require Employees to Install Coronavirus-Tracing Apps like This One from PwC before Coming Back to Work."

wireless connectivity, which these apps would require for cross-referencing identifiers regularly and notifying the exposed. While much of the wireless industry touts the "race to 5G," the next generation of wireless technology, many communities in rural and geographically isolated areas have "no G," as one U.S. senator explained.[70] These communities have no wireless service of any kind, and many providers are loath to invest in them due to high infrastructure costs. Despite the inherent physical distancing in rural areas, these regions are not immune to the pandemic, as demonstrated by the ongoing spread of COVID-19 in meat processing plants in low-density areas like rural Nebraska.

Given these realities, digital exposure notification tools risk leaving behind precisely the people who are most difficult for public health officials to identify, warn, and treat. If public health officials decide to pursue smartphone-based tracing tools, they must address these equity concerns. As described further in our recommendations below, public health officials should confer with minority community leaders in developing a targeted approach toward program implementation, as well as consider investing in digital literacy assistance programs.[71] Digital literacy programs will take time to yield results, but it is still worth beginning that investment now. Further, while manual tracing also presents challenges, the need to reach those communities that may not have the digital literacy skills or smartphone ownership to use digital tools presents yet another reason for public health entities to ensure substantial investment in manual contact tracers. Additional recommendations to mitigate the equity issues posed by digital tracing tools are further discussed below.

[70] "Tester Holds FCC Accountable to Increase Wireless Service in Montana": "'As we work to get 5G across the country, what happens to the places with no G,' Tester said during a Senate Commerce Committee hearing. 'We will never get 1G in Montana if we are focused on bringing 5G to Houston.'"
[71] Landau, Lopez, and Moy, "Importance of Equity in Contact Tracing."

04 Privacy and Cybersecurity/Data Security Threats from Contact Tracing

Privacy Threats

Whenever governments or companies collect personal information about individuals, there are risks that the information will be used for improper secondary purposes, that the information will be abused, including to fuel discrimination, and that there will be a data breach. Therefore, it is of the utmost importance that policymakers and tech companies minimize the amount of personal information collected as part of contact tracing efforts, and safeguard the sensitive health and location information related to coronavirus exposure and disposition under discussion. As discussed above, even manual contact tracing approaches present such privacy threats, since they involve collecting highly personal medical and behavioral information; but these threats are more significant where digital tools collect vast quantities of data, including data on people who never test positive for, or are even exposed to, the coronavirus.

Even where data is only stored or shared in aggregate and anonymized formats, there is a risk of reidentification, a severe privacy risk with real consequences, especially for those who have tested positive for COVID-19. Stigmas and discrimination can develop either when people associate a certain disease with a specific population or toward specific individuals who have been quarantined. Much like in past disease outbreaks, stigmatization has been an issue during the spread of the novel coronavirus in the United States, causing additional stress, fear, and anxiety for certain communities facing discrimination. As Dr. Anthony Fauci and others have pointed out, fear and stigma surrounding positive cases are reminiscent of the AIDS crisis.[72]

For example, across the United States, Asian-Americans have faced discrimination and an uptick in violent attacks during the spread of COVID-19.[73] Similarly, contact tracers in New York City are struggling

[72] Shafer, "Could Lessons From The Early Fight Against AIDS Inform The Coronavirus Response?"
[73] Tavernise and Oppel, "Spit On, Yelled At, Attacked: Chinese-Americans Fear for Their Safety."

to gain the trust of immigrant, Arab, Orthodox Jewish, and other minority communities due to fears that their personal information will be weaponized against them.[74] Additionally, there are already several examples from different countries of the data collected by COVID-19 apps being abused or misused. In South Korea, exposure notifications provided so much detailed information about people who had tested positive that they have turned some citizens into "imperious armchair detectives" who look to track and reidentify individuals.[75] Additionally, the LGBTQ community in Seoul has been the subject of recent tracking, hate, and blame for the latest outbreak.[76] In Norway, the data protection authority ordered the country's public health body to suspend its contact-tracing app due to privacy issues with the app's collection of location data.[77] And Bahrain's BeAware app was used as fodder for state-controlled television: the host of the game show *Are You At Home?* called app users on-air to ask if they were adhering to social distancing guidelines.[78] This stigmatization and fear may also create disincentives for individuals in such communities to even seek testing.

Contact tracing is, by its very nature, intrusive, but digital tools can create additional privacy threats because of the scale of data collected, and the risk that additional entities beyond public health authorities could gain access to the data. Some intrusions into our privacy may be necessary to contain disease—public health professionals may ask infected individuals to look through their phones and recent credit records to help assist in identifying people who may have been exposed. But historically only public health authorities had access to this information, and we have trusted that public health officials' interest is in public health alone.

It is critical that data gathered for contact tracing purposes—whether by traditional methods or through

[74] Eisenberg, "Privacy Fears Threaten New York City's Coronavirus Tracing Efforts."
[75] Thompson, "The Technology That Could Free America From Quarantine."
[76] Kim, "Tracing South Korea's Latest Virus Outbreak Shoves LGBTQ Community into Unwelcome Spotlight."
[77] Manancourt, "Norway Suspends Contact-Tracing App over Privacy Concerns."
[78] Statt, "Gulf States Using COVID-19 Contact Tracing Apps as Mass Surveillance Tools, Report Says."

digital tools such as exposure notification apps—be limited to public health agencies. Neither law enforcement agencies nor technology companies are tasked with securing our public health, and this sensitive personal information should not be shared with them.

Allowing law enforcement access to any of this data would open the door to increased, non-disease-related surveillance, and could permit law enforcement to conduct an end-run around Fourth Amendment safeguards. Further, permitting access to government officials other than public health authorities creates a real risk of mission creep and improper secondary uses of personal data. Once the government obtains new streams of data, it can be very difficult to scale that data collection back and to ensure that it is used properly and in a limited fashion. We should heed these lessons from our experience with the Patriot Act,[79] which created new surveillance authorities post-9/11 and has been a struggle to reform to this very day, nineteen years later. Models taken from counter-terrorism that "fuse" local, state, and national agencies, as was highlighted in the original Safra Center "Roadmap to Pandemic Resilience," are problematic for this reason and require special care and explicit protections for individuals' data.

Tech companies' involvement also raises serious privacy threats and significantly alters the dynamic between public health authorities and the general public. While the majority of Americans trust public health agencies,[80] Americans have largely negative views of tech companies and their impact on society.[81] The business models of many technology companies rely on monetizing user data, which has caused the majority of Americans to feel that they have little control over their personal information.[82] The trove of sensitive health data collected for public health purposes, as well as any location or proximity information collected for exposure notification systems, could also be valuable for commercial

[79] Swire, "Security, Privacy and the Coronavirus: Lessons From 9/11."
[80] Nather, "Exclusive Poll: Public Trusts Health Agencies More than Trump on Coronavirus."
[81] Knight Foundation, "Techlash? America's Growing Concern with Major Technology Companies."
[82] Auxier, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information."

purposes, creating a high risk for secondary uses of this data. Without appropriate guardrails, app developers could use the data for unrelated purposes such as advertising, or sell the data to data brokers who run a lucrative market for personal health information.[83] For example, there is a risk that insurance companies could use the data to deny coverage or raise premiums[84] and pharmaceutical companies could use the data for drug marketing.[85] Already, North Dakota's Care19 app, which collects users' sensitive individual location data, has violated this principle and its own stated privacy protections by sharing location data and unique identifiers (including advertising identifiers) with FourSquare and Google.[86] It will be difficult to earn the public's trust in digital tools without restrictions on such abuses of COVID-19 data, including a ban on use for commercial purposes.

Expanded collection of and access to personal data, whether by government agencies beyond public health authorities or by companies, also increases the risk of harm through data breaches. Indeed, data breaches are a serious risk for the public health authorities and companies collecting and retaining COVID-19 data. The public and private sectors have both been the targets of major security breaches in recent years, such as the OPM data breaches and the Equifax breach. And breaches are so rampant in the healthcare industry that the U.S. Department of Health and Human Services Office for Civil Rights maintains a public list of breaches of unsecured protected health information affecting 500 or more individuals. To mitigate these risks, it is critical to minimize the amount of data collected to that which is actually needed by public health authorities, and to strictly limit what entities have access to the data. Further, all digital contact tracing tools must be designed to meet best practices for securing sensitive health information.

[83] Tanner, "For Sale: Your Medical Records."
[84] Allen, "Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates."
[85] Ornstein, "Big Data + Big Pharma = Big Money."
[86] Melendez, "North Dakota's COVID-19 App Has Been Sending Data to Foursquare and Google."

Regulation limiting the entities authorized to access COVID-19 data and the permitted uses will mitigate the privacy risks posed by digital contact tracing systems. Legitimate interests in using the data for public health research can be preserved while preventing inappropriate secondary uses. As discussed in more detail in the Recommendations section below, we must enact legislation to ensure that the app providers have no commercial interest in our coronavirus data.

Anonymization and Cybersecurity Issues

In addition to developing safeguards to mitigate the risks of improper data use and data breaches, public health authorities will need to adopt practices to guard against a variety of cybersecurity threats. Not just the digital exposure notification apps that are the focus of this paper, but all digital tools that may be used in the process of contact tracing present inherent cybersecurity risks. For example, case management systems are an integral part of a public health organization's response toolkit and, as noted above, digital tools are available to assist public health authorities with these systems. Health agencies must adopt best practices for cybersecurity to protect all these tools, as well as the databases that they produce, and keep them as secure and private as possible. Data security concerns are equally, if not more important in the face of an unprecedented pandemic.

As mentioned above, a central privacy concern in Bluetooth contact tracing technologies is maintaining anonymity of those using the apps, particularly for those users who do eventually test positive for COVID-19 and submit that result to the public health authority operating the tracing system. These people are at the highest risk, both because of the way in which some tracing systems necessarily reveal more data about those who test positive and because of the potential for targeted harassment, stigmatization, and even potential violence against them. Keeping users anonymous is therefore crucial for any proposed digital tracing tool.

The anonymity features of any contact tracing app depend upon what technologies the app uses and how it implements those technologies. For example, some governments are building or have already deployed apps that rely on GPS location information. As noted above, GPS information is not as useful as Bluetooth technology in showing whether two people have possibly transmitted the virus. Additionally, such a system precludes any anonymity because the location information would show the pathways that particular individuals follow, including starting and ending points at their own homes, and because it would deliver absolute location data (as opposed to the relative data that Bluetooth provides).

The cybersecurity threats extend beyond a breach of anonymity. In a recent example, Amnesty International uncovered that Qatar's compulsory exposure notification app EHTERAZ contained security vulnerabilities allowing hackers access to over one million Qatari citizens' sensitive personal information, including names, national IDs, health status, and GPS location data.[87] Moreover, in a June 2020 study, a mobile cybersecurity analysis company assessed seventeen mobile contact tracing apps from around the world on a variety of app security best practices tests and found only one app passed every test, while there was not a single test that even a majority of the apps passed.[88]

Turning to Bluetooth-reliant tools, the Apple/Google proposal is likely to be most prevalent in the United States, not only due to the companies' combined market dominance, but also because it uses cryptography to achieve the exposure alerts without actually turning over names and locations. Despite its focus on retaining anonymity even for those diagnosed with COVID-19, however, there are still some data security concerns with the Apple/Google proposal and with other proposals for digital contact tracing apps. In particular, there are risks that the system could be abused, either by governments seeking to use the data for law enforcement purposes or as another tool for repression in autocratic regimes, or by companies misusing data for commercial purposes to track customer location for advertising or marketing.

[87] Amnesty International UK, "Qatar: 'huge' Security Weakness in COVID-19 Contact-Tracing App."
[88] Goodes, "Report: The Proliferation of COVID-19 Contact Tracing Apps Exposes Significant Security Risks."

In addition, cryptographers and cybersecurity professionals have identified two current lines of attack against the anonymity of the Apple/Google system (and another similar proposal called DP-3T from a coalition of European researchers) that are worth noting. Both involve exploiting the list of infected device identifiers (which each device generates every day and from which can be derived the fifteen-minute rotating identifiers that are broadcast over Bluetooth) that must be distributed in order for each device to determine if they were in close contact with an infected person.

The first attack requires deploying a network of Bluetooth receivers spread around a physical area with enough granularity to follow devices as they move around the area from point to point.[89] While this may seem like a high bar, Bluetooth-enabled urban infrastructure is growing all of the time, including smart meters and street lights. Each receiver could record all of the short-term identifiers it sees over time and put them all in a central database. As people test positive and their infected device identifiers are broadcast to all devices to check for contacts, the database could be used to track which receivers around the area observed the corresponding short-term identifiers and when. In this way, a map of movements of those who test positive could be generated, after which assigning names and addresses is as easy as tracking commutes.

The second attack is even simpler to execute, although it would likely result in identifying fewer subjects than the first.[90] If an attacker hooked a single Bluetooth receiver up to a video camera and stored the identifiers it received over Bluetooth along with the video footage, picking out those who tested positive would be as easy as associating short-term identifiers with frames of the video footage showing those who have tested positive.

[89] Seiskari, Github: Contact Tracing BLE Sniffer POC.
[90] Soltani, Calo, and Bergstrom, “Contact-tracing apps are not a solution to the Covid-19 crisis.”

Both of these attacks are not necessarily mistakes by the authors of the system. Rather they are unavoidable consequences of the need for the system to connect two people together. If it were not for the distribution of the device identifiers of those who test positive, the contact tracing would be impossible. The first of these potential attacks, involving installation of numerous Bluetooth receivers around a wide area, is likely only achievable by government entities like law enforcement. Thus, prohibiting law enforcement access to this data, as discussed elsewhere in this paper, should mitigate this threat. However, the second potential attack could be achieved by a less well-resourced hacker. Thus, these potential breaches of anonymity must be carefully considered and mitigations against them included in any proposal for digital contact tracing tools.

05 Recommendations

Recommendations for Policymakers

We have identified a variety of equity, privacy, and civil liberties concerns that are posed by contact tracing systems, particularly where they rely on digital tools. Policymakers can and should take action to address these concerns, and provide guardrails to ensure that digital tools to support contact tracing are properly designed to provide the information public health officials need, while also protecting individual rights.

While digital tools cannot replace traditional manual methods, they have the potential—if they are implemented with robust safeguards— to assist public health authorities in contact tracing efforts. The most significant hurdle to Bluetooth apps' efficacy will be issues related to adoption, which are deeply intertwined with digital equity issues.

To address these concerns and hopefully improve adoption rates, we recommend that policymakers take steps to: (1) ensure that public health officials develop targeted strategies, possibly including dedicated manual tracers, to address vulnerable populations that are unlikely to be reached by digital apps; (2) encourage partnerships between digital tool developers and community organizations; (3) develop and promote public education campaigns alongside deployment of any apps; (4) take long-overdue steps to close the digital divide; (5) pass comprehensive privacy legislation; and (6) enhance enforcement by the Federal Trade Commission.

Public health authorities should continue to rely upon traditional manual contact tracing methods, and should particularly recognize that digital tools are least likely to be helpful in reaching marginalized and at-risk communities. We recommend that reliance on digital tools be merely supplemental to manual tracing, which will especially be necessary to reach the lower-income and senior populations who are also at highest risk of contracting COVID-19. Immigrant populations, as well, may need more attention from public health authorities. In addition to experiencing lower rates of English proficiency, these communities also have strong concerns about federal policies that disqualify immigrants who have accepted any government benefits from applying for citizenship (the so-called "material support" regulation has been suspended, but community members are often not aware of this) as well as the sharing of data with ICE agents.

Policymakers should encourage partnerships between developers of digital contact tracing tools and community organizations or leaders that represent affected communities. Such partnerships will have crucial inputs in decision-making around the role that app-based contact tracing can play. Developers and providers should consult with community representatives regarding how to design and deploy apps in ways that allay public mistrust. Such partnerships can also be helpful for developing and implementing isolation and treatment plans. For example, the mayor of Chicago created a Racial Equity Rapid Response Team to work with Black and Latino community groups in shaping the response.[91] Maryland's Montgomery County refers Chinese and Spanish speakers to information hotlines run by non-profit organizations. In the hard-hit city of Detroit, a coalition of city agencies, non-profits, and academic institutions has focused on the particular needs of the homeless.[92] Again, such an approach can help to both mitigate risks posed by digital tools, and produce digital tools and practices that are most likely to be used effectively. To achieve these goals, Congress could mandate that funding for tracing regimes be contingent upon partnerships with community organizations. Further, funding to assist tracing efforts should be contingent on localities making equitable and accessible testing and treatment regimes available, again in concert with those most affected.

[91] Malagon, "Latino Communities in Illinois See Uptick in COVID-19 Confirmed Cases: 'Physical Distancing Is a Privilege.'"
[92] Taylor, "Detroit Mobilizes to Protect the Homeless from Coronavirus."

Public health authorities should develop and promote public education campaigns. In order to increase participation, public education campaigns deployed alongside apps will likely be necessary. Early surveys indicate that many Americans of diverse backgrounds are skeptical of the concept of Bluetooth exposure notification apps and are unlikely to participate.[93] Further, as discussed above, there will be many varying approaches throughout the country when it comes to digital tools, as these are state-led efforts. Some states may choose not to use digital tools, some may choose Bluetooth-based approaches and some may, against our recommendations, collect location data. There is already much confusion surrounding both who is developing and providing these tools and what these tools collect and do. Accordingly, each state will need to undertake efforts to correct the many misunderstandings about their particular app offering, and proactively inform the public regarding how they work and what information they collect, if any. These educational efforts will be key to widespread adoption, and demand a concerted, collaborative effort between governments, app providers (and potentially Apple/Google), and community organizations.

The federal government must take long-overdue steps to close the digital divide and connect the millions of people in the United States who lack access to the devices and connectivity upon which any digital tracing system would be built. Congress should pass the Digital Equity Act (S. 1167), a comprehensive bill that would dramatically expand digital literacy training around the country. These training programs are designed to develop precisely the sort of skill sets that people would need to navigate digital apps, Bluetooth functionality, and basic device maintenance.

Furthermore, Congress, in conjunction with the FCC, should significantly expand federal programs to provide emergency connectivity to households that lack internet access during the pandemic. Specifically,

[93] Owens, "Americans Are on Board with Contact Tracing as Long as It Doesn't Involve Cellphone Data"; Timberg et al., "Most Americans Are Not Willing or Able to Use an App Tracking Coronavirus Infections. That's a Problem for Big Tech's Plan to Slow the Pandemic."

Congress should significantly expand funding and eligibility for the Lifeline program, which subsidizes phone and internet service for low-income Americans. The FCC should also work closely with any state that adopts digital exposure notification apps to ensure that Lifeline-supported devices also support such apps, and promulgate any necessary rule changes. Accordingly, the FCC should also abandon its recent proposal to prohibit Lifeline providers from offering free devices in conjunction with Lifeline service.[94] The FCC and Congress should also increase Lifeline's voice and data allowances, at least during the COVID-19 pandemic, to ensure that people can use the program as the literal lifeline it was intended to be. The current caps could deter Lifeline subscribers from downloading contact tracing apps for fear of exceeding data allowances.

Many of these actions are long overdue, but it should be noted that, even in their entirety, these recommendations will not fully ameliorate our equity concerns or bring access to every unserved community. The problems of the digital divide are deep-seated and require long-term investments in infrastructure deployment and affordability that cannot realistically occur in the short-term. Moreover, the only federal agency designed to address these issues—the FCC—has fully retreated from its role over the past three years. In 2017, the FCC deregulated internet providers and wholly abdicated its legal authority to oversee the broadband market. Without this federal cop on the beat, it is difficult to imagine how we can fully close the digital divide in the manner that smartphone-based tracing systems require. Although the enormity of these challenges suggests that we cannot resolve them in the immediate context of the COVID-19 pandemic, the pandemic should provide a new call to action for policymakers. We must begin to implement sorely needed measures to restore FCC enforcement and begin to reduce the digital divide.

[94] FCC, Fifth Report and Order, Memorandum Opinion and Order and Order on Reconsideration, and Further Notice of Proposed Rulemaking; New America's Open Technology Institute, Comments of New America's Open Technology Institute and Public Knowledge.

Congress should pass legislation to provide safeguards and hold governments and companies accountable. Perhaps most crucially, Congress must pass legislation to address the privacy, equity, and civil rights risks posed by digital contact tracing tools. The United States does not have a comprehensive federal privacy law and the inadequacy of the country's sectoral approach to privacy has become particularly pronounced during the pandemic. Significantly, the Health Insurance Portability and Accountability Act (HIPAA) only applies when personal health information is collected by healthcare providers and insurance companies.[95] But when the same information is collected by non-medical entities, such as app providers, HIPAA protections do not apply, leaving Americans' sensitive health data vulnerable in any digital health tools the private sector offers.

As discussed earlier, the pandemic has created privacy threats that cannot wait to be addressed until Congress is able to pass comprehensive privacy legislation, which is unlikely to occur in 2020. Without legal guardrails, the collection of health, proximity, and location data for public health purposes could lead to mission creep by other government entities and threats of commercial use. Therefore, Congress should pursue legislation targeted to the privacy issues specific to public health emergencies, particularly digital exposure notification systems. And state legislatures should fill any gaps Congress leaves to protect the privacy and public health of their residents.

Several different stakeholders—including tech companies, professional associations, and NGOs—have published principles recognizing the need for privacy protections specific to COVID-19.[96] Additionally, a coalition of civil society organizations sent congressional leaders a list of principles addressing the protection of civil rights and privacy of all persons, especially communities of color and other populations

[95] US HHS, Office for Civil Rights. "Covered Entities and Business Associates."
[96] Gilmor, "Principles for Technology-Assisted Contact-Tracing"; AMA, "AMA Privacy Principles"; Brill and Lee, "Preserving Privacy While Addressing COVID-19"; Massé, "Privacy and Public Health: The Dos and Don'ts for COVID-19 Contact Tracing Apps."

who are at high risk for the virus, when considering the deployment of technological measures to combat COVID-19.[97] There is substantial overlap on broad principles, with some distinctions on how those common values should be reflected in legislation. The following principles should serve as a guide to policymakers developing public health emergency privacy legislation.

1. **Meaningful consent:** All participation in contact tracing applications must be voluntary. Voluntariness requires that participation is not a condition for access to public benefits, work, or educational spaces. Companies must obtain meaningful consent to collect and use personal data. The "notice and consent" model that has characterized much of privacy enforcement in the United States fails to protect user privacy under normal conditions and should not be the consent model used for exposure notification systems.[98]
2. **Transparency:** App providers must be fully transparent with users about the type of data collected, the entities that will have access to the data, and how the data will be used. Congress should require notices to be accessible to those with limited English proficiency and to be available in a machine-readable format.
3. **Data Minimization:** App providers should minimize the collection of personal data and only collect the data necessary for specified public health purposes. As noted above, this means that digital tools to assist contact tracing should only collect proximity information, such as Bluetooth data, and not individual location information, such as CSLI or GPS. Further, only apps developed in partnership with public health authorities should be made available to the public, so that only the types of data necessary to support contact tracing are collected.
4. **Limited Retention Period:** The data collected must not be retained by companies or public health authorities indefinitely. Legislation should define a retention period for personal data. The retention period could be a defined period of time, such as every thirty days, or could be tied to a declaration by public health agencies that the emergency has ended. Legislation could also permit longer retention of aggregated anonymized data by public health authorities for research purposes.

[97] New America's Open Technology Institute, "Civil Rights Groups Call for Protection of Democracy and Privacy as Tech Responds to Pandemic."

[98] Park, "How 'Notice and Consent' Fails to Protect Our Privacy."

5. **Prohibition on Secondary Uses:** Personal data must be used for public health purposes only and legislation should prohibit secondary uses. The data must not be used for commercial purposes such as advertising. Data should not be shared with any government entities other than public health authorities. Law enforcement access should be prohibited, including access for pandemic-related purposes, such as the enforcement of stay-at-home orders. Location data must not be used to track individuals.
6. **Data Security:** Companies must maintain best security practices to safeguard the collected data. Such practices include decentralized implementation, de-identification methods like differential privacy, and encryption.
7. **Equity:** Companies must take steps to prevent disparate impacts on certain populations and demographics. Legislation should include a prohibition on discriminatory uses of data related to protected characteristics, including denial of access to education, housing, and employment opportunities. The data must not be used to restrict or deny voting rights.

Legislation rooted in these principles would help to protect the public from the risks that digital tools for contact tracing pose to individual rights. However, if Congress does not pass legislation (or passes weak legislation), there are existing legal frameworks that can be used to hold companies accountable for the privacy practices of contact tracing apps. Both the Federal Trade Commission and state attorneys general have authority to bring enforcement actions against companies that misrepresent their privacy and security practices to users.

The Federal Trade Commission (FTC) and state agencies should be given the resources necessary to hold companies accountable for any privacy violations or other deceptive practices. Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful" and the Commission applies this authority to privacy and security. The FTC typically relies on the deceptiveness prong, bringing privacy cases against companies that do not abide by the representations made to their users in privacy policies or other public-facing documents.[99] All states have similar statutes prohibiting deceptive practices and most also prohibit unfair practices.[100] These state statutes empower their attorneys general to pursue actions against companies' unfair and deceptive privacy and security practices.[101]

If app providers or platforms break the promises made to the public, both the FTC and state attorneys general would have the legal authority to pursue legal action for unfair and deceptive trade practices. For example, Apple and Google have characterized their contact tracing partnership as promoting "Privacy-Preserving Contact Tracing" and have stated that their system does not collect location data and the system is only used by public health authorities. Therefore, if the companies were collecting location data or disclosing data to third parties, the federal and state consumer protection agencies would have grounds for an investigation and potential enforcement actions.

But without legislation establishing legal obligations on exposure notification programs, or more resources for enforcement, the ability of the FTC and state attorneys general to regulate privacy during the pandemic will be severely limited.

Recommendations for Platforms and App Designers

If local governments do choose to move forward with deploying Bluetooth exposure notification apps, as many appear to be, we recommend that platforms and app developers take a number of steps that, even in the absence of legislation, could help ensure privacy is protected, mitigate the equity concerns raised above, and increase participation. These are largely system design recommendations, and many are already required by the Apple/Google API. Where Apple/Google have announced that they require

[99] Keegan and Schroeder, "FTC's Evolving Measures of Privacy Harms."
[100] NCLC, "Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws."
[101] Citron, "Privacy Policymaking of State Attorneys General."

these privacy protections, we urge Apple/Google to not retreat on these important protections down the road, but rather to conduct regular oversight to ensure apps' compliance.

Systems relying on digital tools to aid contact tracing should be decentralized. Data must remain decentralized, meaning data should be stored on individual devices rather than in a centralized server. Germany has already waged an instructive debate on this particular element of the Bluetooth app proposals. In their effort to develop an effective and privacy-protective app for the European Union, the Pan-European-Privacy-Preserving Proximity Tracing team of more than 100 international researchers pushed a centralized approach, through which the pseudonymized proximity data would be stored and processed on a server controlled by a national health authority. However, Germany more recently rejected this approach following an outcry from academics and organizations due to concerns about allowing authorities to amass citizens' data and potential government mission creep.[102] Instead, Germany and some other governments in the E.U. are pursuing a decentralized, more privacy-protecting approach known as the DP-3T proposal, which would also incorporate the other safeguards we recommend for platforms and app designers. However, France has more recently deployed a centralized app named StopCovid (which would not be interoperable with its neighbors' decentralized apps as a result) and that app has not gained substantial uptake. While France's centralized app has only been downloaded by 1.9 million citizens since it launched on June 2,[103] Germany's decentralized app has been downloaded by nearly 10 million Germans since it launched on June 16.[104] This suggests that the low adoption rate in France may stem from the centralized approach, and that the most privacy-protective apps are the best way to improve uptake, and therefore improve effectiveness. Under the decentralized contact tracing infrastructure, identifiers are stored locally on individual devices and are only uploaded with a user's permission after a confirmed COVID-19 diagnosis. U.S. app developers should follow suit.

[102] Lomas, "Germany Ditches Centralized Approach to App for COVID-19 Contacts Tracing."
[103] Braun, "French Contact Tracing App Sent Just 14 Notifications After 2M Downloads."
[104] Seythal, "German Coronavirus Tracing App Downloaded Almost 10 Million Times: Government."

Digital tools must incorporate robust safeguards to protect anonymity of users. Bluetooth-based exposure notification tools rely on phones to generate identifiers that are sent out as beacons and then detected by other phones using the app. Anonymization of these identifiers is key, and the identifiers must be continuously changing, as often as possible, in order to avoid harms related to reidentification. As devices interact via Bluetooth, they will exchange nameless identifiers (again, which will be stored on the devices rather than in a central database). But as outlined above, a significant threat from both a cybersecurity and privacy perspective is reidentification, a threat that can be mitigated by changing identifiers more frequently to make reidentification more challenging. While the central database will keep track of the nameless identifiers (as they change) of the individuals with confirmed cases, the concept is that the database will not be able to track who has been exposed. For example, the Apple/Google API addresses this threat by requiring that identifiers are randomized every fifteen minutes.

Notifications of potential exposure should provide only the minimum information necessary. App providers and governments should work together to ensure that notifications of exposure contain no personally identifiable information. While its collection is not allowed under the Apple/Google infrastructure, location data showing individuals' paths of travel, for instance, can be used to reidentify individuals. Including too much personal or location data in notifications can be problematic, even if not shared with the government.

App designers should partner with local communities to ensure apps are designed to meet community needs. For these system design recommendations, we urge app designers to engage with civil rights and civil liberties advocates as well as community organizations, who can help developers to address community needs and increase reach. Privacy-protective system design should result in higher uptake of the apps, and therefore increased effectiveness. Thus it is important to ensure that the communities most in need of attention—the vulnerable populations at highest risk of coronavirus—have their concerns addressed, and to educate and partner with the relevant communities and organizations in order to spread awareness as to the apps' purposes, privacy protections, and limitations.

Apple and Google should take steps to enforce the safeguards they have announced. Given the predominant market share of Apple and Google, it is likely that exposure notification apps relying on the Apple/Google API will be more widely adopted than other digital tools.[105] As mentioned throughout this section, many of the most crucial privacy protections we recommend are requirements under the Apple/Google API, where apps must: (1) use Bluetooth data only; (2) use frequently-changing anonymous identifiers that only health authorities can temporarily access when necessary; (3) be decentralized; (4) be voluntary; (5) require consent for diagnosis information uploads; and (6) provide transparency to users.[106] Enactment of privacy legislation, as we recommend above, would enable the public to hold these platforms accountable to uphold these privacy safeguards, but with or without such legislation, we strongly urge Apple and Google to conduct regular and conscientious oversight to ensure that app providers strictly comply with these requirements. As the coronavirus battle could rage on for months or potentially years to come, pressure could mount from governments for Apple and Google to scale back these restrictions and allow more access to and collection of data.

Further, Apple and Google may need to consider banning non-API-compliant apps from their app stores to avoid confusion regarding which apps are government-backed and privacy-protective.[107] For example, at present, even though apps using location data are barred from the API, they are allowed in the companies' app stores. In some cases there are multiple apps per state, one complying with the API, one non-compliant.[108] The Apple/Google infrastructure is fairly strong from a privacy perspective, and Apple/Google should maintain these requirements and enforce them by expelling apps that flout the requirements.

[105] Lovejoy, "More Countries Adopting or Switching to Apple/Google Contact Tracing API."
[106] Apple and Google, "Exposure Notification: Bluetooth Specification."
[107] Langley, "Apple and Google Are Facing Pressure from New York's Attorney General to Impose Stricter Privacy Rules on Contact Tracing Apps That Are Currently Flooding Their App Stores."
[108] O'Neill, "Why One US State Will Have Two Coronavirus Tracing Apps."

06 Conclusion

Governments throughout the United States and around the world are turning to contact tracing programs as a critical component of efforts to combat the coronavirus pandemic. The extent to which digital tools can play a meaningful role in expanding the reach of traditional manual contact tracing techniques is not yet clear, and these tools pose a variety of concerns regarding equity, privacy, and civil liberties. Nonetheless, given the scale and impact of this pandemic, digital exposure notification tools may be worth exploring and developing, provided that governments can implement adequate guardrails to control use of these systems.

We have therefore presented a series of recommendations for government officials and for platforms and app developers, to mitigate the risks to privacy and civil liberties, and ensure that use of digital tools for contact tracing is as rights-protective as possible. In addition, we have recommended that public health officials should recognize that digital tools will still exclude vulnerable communities, and should take affirmative steps to both try to reach those communities with digital tools and compensate for the remaining gaps with manual contact tracing.

07 References

Aguilar, David V. Memorandum from David V. Aguilar, Deputy Commissioner, U.S. Customs and Border Protection; subject: U.S. Customs and Border Protection Enforcement Actions at or Near Certain Community Locations; date: January 18, 2013. https://foiarr.cbp.gov/streamingWord.asp?i=1251

Albergotti, Reed, and Drew Harwell. "Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless." *Washington Post*, May 15, 2020. https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/

Allen, Danielle, et al. "Roadmap to Pandemic Resilience: Massive Scale Testing, Tracing, and Supported Isolation (TTSI) as the Path to Pandemic Resilience for a Free Society." Edmond J. Safra Center, COVID-19 Rapid Response Impact Initiative, with support of The Rockefeller Foundation, April 20, 2020. https://ethics.harvard.edu/files/center-for-ethics/files/roadmaptopandemicresilience_updated_4.20.20_1.pdf

Allen, Marshall. "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates." *ProPublica*, March 2, 2020. https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates

AMA. "AMA Privacy Principles." https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf

Amnesty International UK. "Qatar: 'Huge' Security Weakness in COVID-19 Contact-Tracing App." Amnesty International UK, press release, May 26, 2020, https://www.amnesty.org.uk/press-releases/qatar-huge-security-weakness-covid-19-contact-tracing-app

Amnesty International USA. "Contact Tracing App Exposed Sensitive Personal Details of over One Million." *Amnesty International USA*, Press Release, May 26, 2020. https://www.amnestyusa.org/press-releases/contact-tracing-app-security-flaw-exposed-sensitive-personal-details-of-more-than-one-million.

Anderson, Monica, and Andrew Perrin. "Technology Use among Seniors." Pew Research Center: Internet, Technology, May 17, 2017. https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors

Anderson, Monica, and Madhumitha Kumar. "Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption." Pew Research Center, FactTank, May 30, 2020. https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption

Apple and Google. "Exposure Notification: Bluetooth Specification." v1.2, April 2020. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf

References

Apple and Google. “Exposure Notification: Frequently Asked Questions.” v1.0, April 2020. https://blog.google/documents/63/Exposure_Notification_-_FAQ_v1.0.pdf

Apple and Google. “Privacy-Preserving Contact Tracing.” No date. https://www.apple.com/covid19/contacttracing

Auxier, Brooke. “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.” P*ew Research Center: Internet & Technology*, November 15, 2020. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information

Auxier, Brooke. “How Americans See Digital Privacy Issues amid the COVID-19 Outbreak.” Pew Research Center, May 4, 2020. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak

Barry, Ellen. “In a Crowded City, Leaders Struggle to Separate the Sick from the Well.” *New York Times*, April 25, 2020 (updated April 28, 2020). https://www.nytimes.com/2020/04/25/us/coronavirus-chelsea-massachusetts.html

Bourdeaux, Margaret, et al. 2020. “How Human-Centered Tech Can Beat COVID-19 through Contact Tracing.” *The Hill*, April 21, 2020. https://thehill.com/opinion/technology/493648-how-human-centered-technology-can-beat-covid-19-through-contact-tracing.

Bradshaw, Tim. “2 Billion Phones Cannot Use Google and Apple Contact-Tracing Tech.” *Ars Technica*, April 20, 2020. https://arstechnica.com/tech-policy/2020/04/2-billion-phones-cannot-use-google-and-apple-contract-tracing-tech/

Braun, Elisa. “French Contact Tracing App Sent Just 14 Notifications After 2M Downloads.” Politico, June 23, 2020. https://www.politico.eu/article/french-contact-tracing-app-sent-just-14-notifications-after-2-million-downloads/

Brill, Julie, and Peter Lee. “Preserving Privacy While Addressing COVID-19.” *Microsoft on the Issues*, blog posted April 20, 2020. https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/

Bursztyn, Leonardo. “Misinformation During a Pandemic.” University of Chicago, Becker Friedman Institute for Economics, Working Paper, June 15, 2020. https://bfi.uchicago.edu/working-paper/2020-44

CDC. “Coronavirus Disease 2019 (COVID-19): Case Investigation and Contact Tracing; Part of a Multipronged Approach to Fight the COVID-19 Pandemic.” *CDC*, National Center for Immunization and Respiratory Diseases, Division of Viral Diseases, last updated April 29, 2020. https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html

References

CDC. “COVID-19 in Racial and Ethnic Minority Groups” Centers for Disease Control and Prevention, last reviewed June 4, 2020. https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/racial-ethnic-minorities.html

CDC. “U.S. Public Health Service Syphilis Study at Tuskegee: The Tuskegee Timeline.” Last reviewed March 2, 2020. https://www.cdc.gov/tuskegee/timeline.htm

Citron, Danielle Keats. “The Privacy Policymaking of State Attorneys General.” *Notre Dame Law Review*, 92, no. 2 (2017): 747–816. https://scholarship.law.nd.edu/ndlr/vol92/iss2/5/

Confessore, Nicholas. “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.” *New York Times*, November 15, 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Coombs, Bertha. “Microsoft and UnitedHealth Offer Companies Free App to Screen Employees for Coronavirus.” *CNBC*, May 15, 2020. https://www.cnbc.com/2020/05/15/microsoft-and-unitedhealth-offer-companies-free-app-to-screen-employees-for-coronavirus.html

DP-3T Coalition. Decentralized Privacy-Preserving Proximity Tracing. https://github.com/DP-3T/documents.

Eisenberg, Amanda. “Privacy Fears Threaten New York City’s Coronavirus Tracing Efforts.” *Politico*, June 4, 2020. https://www.politico.com/states/new-york/albany/story/2020/06/04/privacy-fears-threaten-new-york-citys-coronavirus-tracing-efforts-1290657

FCC. “FCC Proposes over $200 Million in Fines against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data.” Federal Communications Commission, Press Release, February 28, 2020. https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf

FCC. “Fifth Report and Order, Memorandum Opinion and Order and Order on Reconsideration, and Further Notice of Proposed Rulemaking, WC Docket No. 17-287, WC Docket No. 11-42, and WC Docket No. 09-197” (Rel. Nov. 14, 2019). https://docs.fcc.gov/public/attachments/FCC-19-111A1.pdf

Fields, Jessica. “We Are Leaving Older Adults out of the Digital World.” *TechCrunch*, May 5, 2019. https://techcrunch.com/2019/05/05/we-are-leaving-older-adults-out-of-the-digital-world/

Fox, Maggie. “‘We Need an Army’: Hiring of Coronavirus Trackers Is Likely Set to Soar.” *STAT*, April 13, 2020. https://www.statnews.com/2020/04/13/coronavirus-health-agencies-need-army-of-contact-tracers.

Franklin, Sharon Bradford. “The Right and Wrong Ways to Use Location Data in the Pandemic.” *Slate*, April 8, 2020. https://slate.com/technology/2020/04/coronavirus-location-data-heat-maps-privacy.html

References

Fussell, Sidney, and Will Knight. "The Apple-Google Contact Tracing Plan Won't Stop Covid Alone." *Wired,* April 14, 2020. https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone

Gilmor, Daniel Kahn. "Principles for Technology-Assisted Contact-Tracing." ACLU White Paper, April 16, 2020. https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing

Goodes, Grant. "Report: The Proliferation of COVID-19 Contact Tracing Apps Exposes Significant Security Risks." *Guardsquare*, June 18, 2020. https://www.guardsquare.com/en/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant-security-risks

Google. "Exposure Notification API Launches to Support Public Health Agencies." *Google*, The Keyword, May 20, 2020. https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches

Greiner, Ashley L., et al. "Addressing Contact Tracing Challenges—Critical to Halting Ebola Virus Disease Transmission." *International Journal of Infectious Diseases* 41 (Nov. 2015): 53–55. https://www.sciencedirect.com/science/article/pii/S1201971215002593

Hall, Peter. "ICE Criticized for Arrest at Scranton Hospital." *The Morning Call*, March 16, 2020. https://www.mcall.com/news/pennsylvania/mc-nws-pa-ice-immigrant-arrest-hospital-scranton-coronavirus-20200316-3itqa24pdfau3kjnkm62jcdsai-story.html

Hardeman, Rachel R., et al. "Structural Racism and Supporting Black Lives: The Role of Health Professionals." *New England Journal of Medicine*, 375, no. 22 (2016): 2113–15. https://www.nejm.org/doi/10.1056/NEJMp1609535

Haskins, Carole, et al. "We Need An 'Army' Of Contact Tracers To Safely Reopen The Country. We Might Get Apps Instead." *BuzzFeed News*, April 29, 2020. https://www.buzzfeednews.com/article/carolinehaskins1/coronavirus-contact-tracing-google-apple.

Hogan, Alex. "How Much of the Coronavirus Does It Take to Make You Sick? The Science, Explained." *STAT*, April 14, 2020. https://www.statnews.com/2020/04/14/how-much-of-the-coronavirus-does-it-take-to-make-you-sick

Holder, Sarah. "Who Wants to Be a Contact Tracer?" *CityLab*, May 12, 2020. https://www.citylab.com/solutions/2020/05/contact-tracing-coronavirus-cases-data-jobs-technology-apps/611119

Horowitz, Jason, and Adam Satariano. "Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation." *New York Times*, June 16, 2020. https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html

Hub Staff. "Asymptomatic Spread Makes COVID-19 Tough to Contain." Johns Hopkins University, *The Hub*, May 12, 2020. https://hub.jhu.edu/2020/05/12/gigi-gronvall-asymptomatic-spread-covid-19-immunity-passports/

References

ICE. “ICE Guidance on COVID-19.” U.S. Immigration and Customs Enforcement, https://www.ice.gov/coronavirus

Johnson, Bobbie. “Nearly 40% of Icelanders Are Using a Covid App—and It Hasn’t Helped Much.” *MIT Technology Review*, May 11, 2020. https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing

Kahn, Jeffrey, and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. *Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance*. Baltimore: Johns Hopkins University Press, 2020. https://muse.jhu.edu/book/75831

Keegan, Cobun, and Calli Schroeder. “The FTC’s Evolving Measures of Privacy Harms.” *Journal of Law*, Economics, & Policy 15, no. 1 (Winter): 19–40. https://jlep.net/home/wp-content/uploads/2019/01/JLEP-Volume-15-1.pdf

Kim, Min Joo. “Tracing South Korea’s Latest Virus Outbreak Shoves LGBTQ Community into Unwelcome Spotlight.” *Washington Post*, May 11, 2020. https://www.washingtonpost.com/world/asia_pacific/tracing-south-koreas-latest-virus-outbreak-shoves-lgbtq-community-into-unwelcome-spotlight/2020/05/11/0da09036-9343-11ea-87a3-22d324235636_story.html

Knight Foundation. “Techlash? America’s Growing Concern with Major Technology Companies.” Knight Foundation Trust, Media and Democracy initiative, with Gallup, Report, 2020. https://knightfoundation.org/wp-content/uploads/2020/03/Gallup-Knight-Report-Techlash-Americas-Growing-Concern-with-Major-Tech-Companies-Final.pdf

Kurtzman, Laura. “UCSF Partners with State to Develop Public Health Workforce for COVID-19 Response.” *University of California San Francisco*, May 4, 2020. https://www.ucsf.edu/news/2020/05/417346/ucsf-partners-state-develop-public-health-workforce-covid-19-response.

Landau, Susan, Christy E. Lopez, and Laura Moy. “The Importance of Equity in Contact Tracing.” *Lawfare*, May 1, 2020. https://www.lawfareblog.com/importance-equity-contact-tracing

Landau, Susan. “Location Surveillance to Counter COVID-19: Efficacy Is What Matters.” *Lawfare*, March 25, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters

Landau, Susan. “Looking Beyond Contact Tracing to Stop the Spread.” *Lawfare*, April 10, 2020. https://www.lawfareblog.com/looking-beyond-contact-tracing-stop-spread

Langley, Hugh. “Apple and Google Are Facing Pressure from New York’s Attorney General to Impose Stricter Privacy Rules on Contact Tracing Apps That Are Currently Flooding Their App Stores.” *Business Insider*, June 15, 2020. https://www.businessinsider.com/ny-attorney-general-apple-google-contact-tracing-app-rules-2020-6

References

Lauer, Stephen A., et al. "The Incubation Period of Coronavirus Disease 2019 (COVID-19) From Publicly Reported Confirmed Cases: Estimation and Application." *Annals of Internal Medicine* 172, no. 9 (2020): 577–82. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7081172/

Leith, Douglas and Farrell, Steven. "Coronavirus Contact Tracing: Evaluating the Potential of Using Bluetooth Received Signal Strength for Proximity Detection." Trinity Colleg Dublin, Ireland, School of Computer Science and Statistics, May 6, 2020. https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf

Leswing, Kif. "Companies Could Require Employees to Install Coronavirus-Tracing Apps like This One from PwC before Coming Back to Work." *CNBC*, May 6, 2020. https://www.cnbc.com/2020/05/06/pwc-is-building-coronavirus-contact-tracing-software-for-companies.html

Lomas, Natasha. "Germany Ditches Centralized Approach to App for COVID-19 Contacts Tracing." *TechCrunch*, April 27, 2020. https://techcrunch.com/2020/04/27/germany-ditches-centralized-approach-to-app-for-covid-19-contacts-tracing/

Lovejoy, Ben. "More Countries Adopting or Switching to Apple/Google Contact Tracing API." *9to5Mac*, June 4, 2020. https://9to5mac.com/2020/06/04/switching-to-apple/

Malagon, Elvia. "Latino Communities in Illinois See Uptick in COVID-19 Confirmed Cases: 'Physical Distancing Is a Privilege.'" *Chicago Tribune*, May 6, 2020. https://www.chicagotribune.com/coronavirus/ct-coronavirus-spread-latino-neighborhoods-chicago-20200506-cq2cyli5sfhldjmpwtt2vvtmd4-story.html

Manancourt, Vincent. "Norway Suspends Contact-Tracing App over Privacy Concerns." *Politico*, June 15, 2020. https://www.politico.eu/article/norway-suspends-contact-tracing-app-over-privacy-concerns

Massé, Estelle. "Privacy and Public Health: The Dos and Don'ts for COVID-19 Contact Tracing Apps." *Access Now*, May 4, 2020. https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps

McQuate, Sarah. "A Contact-Tracing App That Helps Public Health Agencies and Doesn't Compromise Your Privacy." *UW News*, April 22, 2020. https://www.washington.edu/news/2020/04/22/a-contact-tracing-app-that-helps-public-health-agencies-and-doesnt-compromise-your-privacy

Melendez, Steven. "North Dakota's COVID-19 App Has Been Sending Data to Foursquare and Google." *Fast Company*, May 21, 2020. https://www.fastcompany.com/90508044/north-dakotas-covid-19-app-has-been-sending-data-to-foursquare-and-google

MIT Media Lab. "Safe Paths: A Privacy-First Approach to Contact Tracing." *MIT News*, April 10, 2020. https://news.mit.edu/2020/safe-paths-privacy-first-approach-contact-tracing-0410

References

Morse, Jack. “North Dakota Launched a Contact-Tracing App. It’s Not Going Well.” *Mashable*, May 6, 2020. https://mashable.com/article/north-dakota-contact-tracing-app

Morton, John. Memorandum from John Morton, Director, U.S. Immigration and Customs Enforcement, to Field Office Directors, et al.; subject: Enforcement Actions at or Focused on Sensitive Locations; date: October 24, 2011. https://www.ice.gov/doclib/ero-outreach/pdf/10029.2-policy.pdf

Movement for Black Lives. “National Demands for COVID-19.” https://m4bl.org/covid-19-platform/#healthcarenotwarfare

Mozur, Paul, et al. “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags.” *New York Times*, March 1, 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Nadi, Aliza. “Inside an ‘Army’ of COVID-19 Contact Tracers in Massachusetts.” *NBC News*, April 30, 2020. https://www.nbcnews.com/news/us-news/inside-army-covid-19-contract-tracers-massachusetts-n1193526.

Nather, David. “Exclusive Poll: Public Trusts Health Agencies More than Trump on Coronavirus.” *Axios*, March 17, 2020. https://www.axios.com/coronavirus-axios-surveymonkey-poll-6cec0f29-bff2-4d1e-bcc8-811e7981f0fe.html

NCLC. “Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws.” National Consumer Law Center, March 2018. https://www.nclc.org/images/pdf/udap/udap-report.pdf

New America Foundation, Open Technology Institute. “Civil Rights Groups Call for Protection of Democracy and Privacy as Tech Responds to Pandemic.”. New America Foundation, Open Technology Institute, press release, June 11, 2020. https://www.newamerica.org/oti/press-releases/civil-rights-groups-call-protection-democracy-and-privacy-tech-responds-pandemic/

New America’s Open Technology Institute. “Comments of New America’s Open Technology Institute and Public Knowledge, before the Federal Communications Commission,” January 27, 2020. https://newamericadotorg.s3.amazonaws.com/documents/OTI_and_PK_Lifeline_FNPRM_Comments.pdf

Newton, Casey. “Why Bluetooth Apps Are Bad at Discovering New Cases of COVID-19.” *The Verge*, April 10, 2020. https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health

O’Donnell, Jaybe. “Coronavirus: Some Fear Black People Won’t Get Vaccine. Here’s Why.” *USA Today*, April 19, 2020. https://eu.usatoday.com/story/news/health/2020/04/19/coronavirus-vaccine-black-americans-prevention/5146777002

O’Neill, Patrick Howell, et al. “A Flood of Coronavirus Apps Are Tracking Us. Now It’s Time to Keep Track of Them.” *MIT Technology Review*, May 7, 2020. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker

References

O'Neill, Patrick Howell. "Why One US State Will Have Two Coronavirus Tracing Apps." *MIT Technology Review*, May 20, 2020. https://www.technologyreview.com/2020/05/20/1002042/why-one-us-state-will-have-two-coronavirus-tracing-apps

Ornstein, Charles. "Big Data + Big Pharma = Big Money." *ProPublica*, January 10, 2014. https://www.propublica.org/article/big-data-big-pharma-big-money

Osterholm, Michael T., and Mark Olshaker. "Let's Get Real About Coronavirus Tests." *New York Times*, April 28, 2020. https://www.nytimes.com/2020/04/28/opinion/coronavirus-testing.html

Owens, Caitlin. "Americans Are on Board with Contact Tracing as Long as It Doesn't Involve Cellphone Data." *Axios*, May 19, 2020. https://www.axios.com/contact-tracing-coronavirus-cell-phone-data-privacy-dbf2f9f6-f06b-4857-ba01-7cb076946573.html

Park, Claire. "How 'Notice and Consent' Fails to Protect Our Privacy." New America Foundation, Open Technology Institute, blog posted March 23, 2020. https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy

Pearce, Katie. "Johns Hopkins Launches Online Course to Train Army of Contact Tracers to Slow Spread of COVID-19." *The Hub*, May 11, 2020. https://hub.jhu.edu/2020/05/11/free-contact-tracing-course-johns-hopkins

PEPP-PT. "Pan-European Privacy Preserving Proximity Tracing." https://www.pepp-pt.org (accessed June 5, 2020).

Pew Research Center. "Mobile Fact Sheet." Pew Research Center: Internet & Technology, June 2, 2020. https://www.pewresearch.org/internet/fact-sheet/mobile

Pillion, Dennis. "Alabama Balances Privacy against Accuracy in Contact Tracing App." AL.com, May 29, 2020. https://www.al.com/news/2020/05/alabama-balances-privacy-against-accuracy-in-new-contact-tracing-app.html

Qian, Hua, et al. "Indoor Transmission of SARS-CoV-2." 2020. *medRxiv*, preprint, April 7, 2020. https://www.medrxiv.org/content/10.1101/2020.04.04.20053058v1

Ross, Janell. "From White Conservatives to Black Liberals, Coronavirus Misinformation Poses Serious Risks." *NBC News*, May 2, 2020. https://www.nbcnews.com/news/nbcblk/coronavirus-misinformation-crosses-divides-infect-black-social-media-n1198226

Sarkesian, Lauren. "Amid Reopenings, Technology Alone Won't Stop the Coronavirus." *Just Security*, April 29, 2020. https://www.justsecurity.org/69919/as-the-u-s-risks-reopening-for-business-technology-alone-wont-stop-the-coronavirus

References

Schaeffer, Katherine. “Nearly Three-in-Ten Americans Believe COVID-19 Was Made in a Lab.” *Pew Research Center*, April 8, 2020. https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab

Seiskari, Otto. Github: Contact Tracing BLE Sniffer PoC. https://github.com/oseiskar/corona-sniffer.

Sellers, Frances Stead, and Ben Guarino. “Contact Tracing Is ‘Best’ Tool We Have until There’s a Vaccine, Health Experts Say.” *Washington Post*, June 14, 2020. https://www.washingtonpost.com/national/contact-tracing-is-best-tool-we-have-until-theres-a-vaccine-say-health-experts/2020/06/13/94f42ffa-a73b-11ea-bb20-ebf0921f3bbd_story.html

Seythal, Thomas. “German Coronavirus Tracing App Downloaded Almost 10 million Times: Government.” *Reuters*, June 19, 2020. https://www.reuters.com/article/us-health-coronavirus-germany-apps/german-coronavirus-tracing-app-downloaded-almost-10-million-times-government-idUSKBN23Q1LP

Shafer, Scott. “Could Lessons from The Early Fight Against AIDS Inform The Coronavirus Response?” *NPR*, April 10, 2020. https://www.npr.org/sections/health-shots/2020/04/10/831045850/could-lessons-from-the-early-fight-against-aids-inform-the-coronavirus-response

Simmons-Duffin, Selena. 2020. “States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago.” *NPR*, Morning Edition, April 28, 2020 (updated May 7, 2020). https://choice.npr.org/index.html?origin=https://www.npr.org/sections/health-shots/2020/04/28/846736937/we-asked-all-50-states-about-their-contact-tracing-capacity-heres-what-we-learne

Simpson, Erin, and Adam Conner. “Digital Contact Tracing To Contain the Coronavirus.” *Center for American Progress*, April 22, 2020. https://www.americanprogress.org/issues/technology-policy/news/2020/04/22/483521/digital-contact-tracing-contain-coronavirus

Soltani, Ashkan, Ryan Calo, and Carl Bergstrom. “Contact-tracing apps are not a solution to the Covid-19 crisis.” Brookings Institute, *Tech Stream*, April 27, 2020. https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/

Statt, Nick. “Gulf States Using COVID-19 Contact Tracing Apps as Mass Surveillance Tools, Report Says.” *The Verge*, June 16, 2020. https://www.theverge.com/2020/6/16/21293363/covid-19-contact-tracing-bahrain-kuwait-mass-surveillance-tools-privacy-invasion

Swire, Peter. “Security, Privacy and the Coronavirus: Lessons From 9/11.” *Lawfare*, March 24, 2020. https://www.lawfareblog.com/security-privacy-and-coronavirus-lessons-911

Talev, Margaret. “Americans Highly Resistant to Participating in a Contact Tracing Program.” *Axios*, May 12, 2020. https://www.axios.com/axios-ipsos-coronavirus-week-9-contact-tracing-bd747eaa-8-fa1-4822-89bc-4e214c44a44d.html

References

Tanner, Adam. “For Sale: Your Medical Records.” *Scientific American* 314, no. 2 (Jan. 2016): 26–27. https://www.researchgate.net/publication/291373859_For_Sale_Your_Medical_Records

Tavernise, Sabrina, and Richard A. Oppel Jr. “Spit On, Yelled At, Attacked: Chinese-Americans Fear for Their Safety.” *New York Times*, June 2, 2020. https://www.nytimes.com/2020/03/23/us/chinese-coronavirus-racist-attacks.html

Taylor, Kimberly Hayes. “Detroit Mobilizes to Protect the Homeless from Coronavirus.” *Curbed Detroit*, April 27, 2020. https://detroit.curbed.com/2020/4/27/21238550/detroit-homeless-shelter-coronavirus-covid

TCN Coalition. “About TCN.” https://tcn-coalition.org/ (accessed June 5, 2020).

TestAndTrace. “What U.S. States Are Ready To Test & Trace?” *#TestAndTrace*, June 1, 2020. https://testandtrace.com/state-data/

Tester, Jon. “Tester Holds FCC Accountable to Increase Wireless Service in Montana.” Jon Tester, U.S. Senator for Montana, press release, August 16, 2018. https://www.tester.senate.gov/?p=press_release&id=6354

Thompson, Derek. “The Technology That Could Free America From Quarantine.” *The Atlantic*, April 7, 2020. https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577

Timberg, Craig, Drew Harwell, and Alauna Safarpour. “Most Americans Are Not Willing or Able to Use an App Tracking Coronavirus Infections. That’s a Problem for Big Tech’s Plan to Slow the Pandemic.” *Washington Post*, April 29, 2020. https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/

U.S. Department of Health and Human Services, Office for Civil Rights. “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.” https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. HHS, Office of Civil Rights. “Covered Entities and Business Associates.” Last reviewed June 16, 2017. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

Yin, Alice. “Cook County Board President Toni Preckwinkle Vetoes ‘Extraordinarily Bad’ Plan to Share Coronavirus-Positive Addresses with First Responders, a First in Her Tenure.” *Chicago Tribune*, May 27, 2020. https://www.chicagotribune.com/coronavirus/ct-coronavirus-cook-county-board-address-sharing-preckwinkle-veto-20200526-jrk5374d4jfstjnhkha7tb2qmu-story.html