The year 2020 has witnessed the overlapping public health crises of a global pandemic and ongoing police violence—both of which underscore the devastating effects of systemic racism in the United States. In response to the murders of George Floyd, Breonna Taylor, Tony McDade, and countless other Black and Brown people at the hands of police and other agents of state violence, organizers and activists across the country have taken to the streets demanding justice, Black liberation, and an end to systemic racism. Meanwhile, as COVID-19 continues to devastate communities across the country, data from the Centers for Disease Control and Prevention (CDC) show that Black, Latinx, and Indigenous people are around two-and-a-half times more likely to contract the virus than white people, and around five times more likely to be hospitalized. Black people are two times more likely to die from COVID-19 than white people. While case rate data of Native Hawaiian and Pacific Islander people are not disaggregated from the broader category of “Asian” in CDC data, data from Alaska reveal that this demographic is thirty times more likely than white people to be hospitalized and twelve times more likely to die from COVID-19 in the state. In Washington and Oregon, confirmed case rates for Native Hawaiian and Pacific Islander people are nine times and three times higher, respectively, than those of white people.

Research demonstrates that these inequities are due to long-standing structural racism, including “historic racial segregation and their inextricable downstream effects on the differential quality and distribution of housing,”
transportation, economic opportunity, education, food, air quality, health care, and beyond. The inequities created by structural racism reverberate into carceral facilities—including prisons, jails, and detention centers—where estimates suggest that COVID-19 infection rates are at least five-and-a-half times higher than among the general population.

Policing is another area where long-standing forms of systemic and structural racism are deeply pronounced. Black and Indigenous people are respectively over two and three times more likely to be killed by police than white people. Even in the absence of violence, Black and Brown communities are heavily policed. For example, a 2013 district court ruling revealed that between 2004 and 2012, 83 percent of New York City Police Department (NYPD) stops were of Black and Latinx residents, while these communities make up only 52 percent of the general population in the city. As public health departments try to manage the COVID-19 pandemic, many local jurisdictions are misguidedly turning to police to enforce public safety, such as stay-at-home orders, mask-wearing, and social distancing. Police enforcement of public health orders disproportionately targets historically and structurally marginalized people, particularly Black and Brown people. For example, in New York, data from the NYPD between March and May 2020 reveal that 93 percent of “COVID-related arrests” (e.g., “violating emergency measures” or failure to socially distance) were of people of color, despite this demographic making up around half of the city’s population.

Surveillance as a tool for policing Black and Brown communities also creates tension in the current global sociopolitical moment. While the rise of surveillance technology allows public health departments to track the spread of the virus through communities, it also increases the potential risk of police further targeting and criminalizing Black and Brown people and, in the current moment of increased social activism, specifically tracking activists of color. At an extreme end, a judge in Louisville ordered ankle monitors for people with confirmed COVID-19 cases who refused to self-isolate. Meanwhile, police departments in Daytona Beach, Florida, and Westport, Connecticut, had proposed using drones that can detect body temperatures to track COVID-19, though privacy advocates managed to quash the idea. While the use of these technologies may be limited to COVID-19 prevention thus far (as far as we know), there are few protections in place that would prevent their more widespread future use.

However, almost every public health department, at the recommendation of the CDC, is tracking the spread of COVID-19 with contact tracing—a process by which health departments identify, monitor, and support those who have been exposed to the virus via close contact with a confirmed case. Contact tracing is not a new tool; it has been effective at controlling epidemics since the early twentieth century. The process is managed at the state, tribal, local, and territorial levels, and each state applies CDC guidelines according to its own context. Some health departments are contracting with private tech companies like Apple and
Google, who are creating phone apps that use Bluetooth technology to detect whether someone comes within six feet of a confirmed case and send an automatic notification to the individual. Others are using case management platforms, where health department employees are notified of positive cases by testing sites, call the person with a confirmed case to obtain information about them and any contacts they have been within six feet of, and then notify those potential contacts without revealing the name of the initial case. Other health departments are using some combination of these methods.

In early June 2020, at the start of the renewed uprisings for Black liberation, the public safety commissioner in Minnesota mistakenly declared that the police department was using contact tracing to track those who had been arrested at protests. Public health authorities later clarified that this was not the case, and that the language of “contact tracing” was being misused. However, there are still no mandated protections in place to prevent police from using the tools of public health technology to target and police communities. At least two-thirds of states report that they are sharing these data with first responders, including police, to protect them from risk of being exposed to COVID-19, and at least ten of those states are also sharing identifiable information, such as people’s names. For Black and Brown communities, especially those who are actively involved in protesting and activism, this collaboration between public health and police is particularly concerning. While there is not one clear solution to prevent both further spread of COVID-19 and privacy violations, public health departments can learn from history and find ways to center interventions on belonging—defined as the ability to shape and make demands of social and political structures—particularly for those most disproportionately impacted by the virus.

How Did We Get Here?: Police Power, Individual Rights, and Public Health

There is a long-standing tension between protecting public health and protecting individual liberties in the context of controlling epidemics. While this tension is arising during the current moment of the COVID-19 pandemic in the demands of those who do not want to wear masks and who want to reopen all businesses, it is important to consider whose individual liberty is at stake and in what ways. The demands for economic reopening and antimasking are inextricably linked to social exclusion, racism, and othering, putting the lives of others at risk, including disproportionately those who are already historically and structurally marginalized. In contrast, the demand for individual rights and privacy from privacy experts as contact tracing methods are developed support the idea of belonging, particularly as it applies to activists attempting to create inclusive and antiracist social change. This distinction is critical to observe in the context of the current moment.
While the last decade has seen increasing public recognition of policing as a public health issue, public health officials have historically used police power as a tool for managing disease. For example, in 1905, the Massachusetts Supreme Court decided in *Jacobson v. Massachusetts* that the use of police power and the limiting of individual liberties for the protection of public health was justified. During this time of a smallpox epidemic in Massachusetts, the Board of Health assembled “virus squads,” which consisted of physicians and police traveling into the community together to forcibly vaccinate those who had not been vaccinated. By the end of 1904, a case was brought before the Supreme Court around the issue of compulsory vaccination. The defendant was Swedish Lutheran pastor Henning Jacobson, who objected to compulsory vaccination on the grounds that it violated the individual liberties secured in the Preamble, the Fourteenth Amendment, and the spirit of the Constitution. Jacobson was against vaccination because he had had a negative experience as a child, which he described in his argument as “great and extreme suffering, for a long period.” Ultimately, the Supreme Court upheld the power of the state to enforce compulsory vaccination using police power, in the name of protection of public health. The only limits placed on this power in the decision was when regulations were “arbitrary and oppressive,” with no further definition of those terms.

In more recent history, and building off the precedent of *Jacobson v. Massachusetts*, faculty at the Center for Law and the Public’s Health (a joint initiative at Georgetown and Johns Hopkins universities) drafted the Model State Emergency Health Powers Act (MSEHPA) in response to the events of September 11, 2001, and ensuing mailings containing anthrax that targeted news media offices and congresspeople. The purpose of MSEHPA was to grant public health powers to state and local authorities in case of public health emergencies, including bioterrorism or epidemics. Many states have incorporated parts of MSEHPA into state legislation, though without much consistency. Among other things, the act includes provisions that, during a public health emergency, protected health information should only be accessible to those providing medical treatment to the individual, those conducting epidemiologic research, and those investigating the mechanism of transmission. Additionally, one of the legislative findings in MSEHPA is that “the rights of people to liberty, bodily integrity, and privacy must be respected to the fullest extent possible consistent with maintaining and preserving the public’s health and security.” Another finding highlights the principles of justice and antidiscrimination, urging states to act fairly and equitably to all individuals. The principles outlined in MSEHPA and in *Jacobson v. Massachusetts* provide guidance for pandemic management today, during COVID-19.

There are also historical examples of successful epidemic management using pathways for protecting public health that did not rely on police power. For example, in 1947, New York City faced its own
smallpox epidemic. The city launched a mass vaccination campaign, providing free and voluntary vaccinations through private physicians and the health department, which was advertised far and wide. A comprehensive communication strategy was put in place that involved multiple daily press conferences, radio shows, and publicity of numbers vaccinated in the daily newspaper.\textsuperscript{24} Medical historian Judith Walzer Leavitt notes, “There was a perception of, and also a reality of, honesty and justice from the Health Department and from the city government at this time, in large part because people felt they were being informed of every detail as events unfolded.”\textsuperscript{25} The vaccination campaign was buttressed by contact tracing: epidemiologists traced any known cases of smallpox to their origins and ensured anyone who the infected person may have contacted received a vaccine. Though the health department had the legal authority to use police power to require vaccination, it was not needed. This example should be instructive: transparency, clear communication, and free access to health care can create the conditions under which both public health and individual civil liberties can be protected.

Another lesson to be learned is from HIV/AIDS activism, although care should be exercised in drawing comparisons between HIV and COVID-19 as there are fundamental differences between them. Contact tracing has been used historically to manage the spread of HIV/AIDS by identifying and notifying sexual partners of those who are HIV positive. Stigmatization, discrimination, and criminalization of those who are HIV positive and of those who use drugs made it risky to share a list of sexual partners or partners who injected drugs using the same needle. In the 1980s, many states enacted laws that criminalized people who were HIV positive for exposing others to the virus. Today, thirty-four states still have laws in place that criminalize people living with HIV,\textsuperscript{26} disproportionately targeting people of color, those who use drugs, and LGBTQ+ people.

If health departments share information obtained from contact tracing with police, it could be used to arrest and prosecute those who are HIV positive. Perhaps the most known instance of this was in the case of Nushawn Williams, a young man in New York who tested positive for HIV after contact tracing identified him as a former sexual partner of a woman with chlamydia. Once he tested positive, contact tracers began to reach out to more of Williams’s sexual partners, eventually getting a court order to name him a “clear and imminent danger to the public health” and setting off a months-long search to arrest Williams in 1997 for exposing several women to HIV.\textsuperscript{27} Williams served 12 years in prison and is now under mandated civil confinement in New York. His case set off a widespread debate over the criminalization of HIV and the lack of privacy protections for those who test positive. Consequently, privacy protections around partner notification became and remain a real concern for those directly impacted, and for HIV/AIDS activists. Legal and ethical debates continue around physicians’ duty to warn versus
their commitment to doctor-patient confidentiality, and the privacy of those with HIV is still largely unprotected.28

Privacy Concerns with Digital Contact Tracing for COVID-19

With the highly infectious nature of COVID-19, contact tracing is a huge and labor-intensive task. Prior to COVID-19, the US had about 2,200 contact tracers working in state and local health departments.29 The American Medical Association, the Association of State and Territorial Health Officials, and others estimate that the US needs at least 100,000 contact tracers to properly control the pandemic.30 Given the costs of manual contact tracing and case management, it is no wonder that countries are looking to technology to automate the process.

Some countries, like South Korea, are using cell phone geolocation data through phone apps, cell phone towers, or Global Positioning System to track the movements of positive cases.31 This serves the dual purpose of ensuring positive cases stay quarantined and identifying other cell phone users nearby who might have been exposed to the virus. Other countries, like Singapore, are using Bluetooth technology to detect whether someone is within six feet of a confirmed positive case and then notify the user of potential exposure. Google and Apple have built on this Bluetooth technology, creating a system for iPhones and Androids called Exposure Notification. The opt-in system creates a new Temporary Exposure Key for each phone daily and a Rolling Proximity Identifier every ten to twenty minutes. When someone is near another phone user with Exposure Notification enabled, their phones exchange these identifiers and store the data, including how long the interaction lasted and how strong the signal was. If a person tests positive for COVID-19, they can send their Temporary Exposure Keys from the last two weeks to the health department, which can then access the identifier data from all other phones that came into contact with the positive case.

While Apple and Google say they have put protections in place to ensure that the data are unidentifiable and privacy is maintained, there are still risks involved with app-based contact tracing and with tech companies’ involvement in public health surveillance. Public health departments and tech companies can put as many privacy protections in place as possible and still not be able to guarantee total privacy. For example, because the Apple/Google platform is constantly transmitting identifier keys via Bluetooth, the time and location data from that platform could be paired with other surveillance techniques (e.g., a video camera at a location near a protest) to identify someone if they later test positive for the virus.32 Such linking of surveillance data could be done by law enforcement or by employers, landlords, and advertising agencies for their own gains.33 The involvement of tech companies like Palantir—which is notorious for
helping the federal government track immigrants and now has over $42 million in contracts with the federal government for pandemic response—adds its own dangers to the safety and security of activists, people of color, and people who are undocumented.\textsuperscript{34}

As noted above, manual methods of contact tracing via public health departments also require more explicit and well-defined privacy protections to prevent identifiable health and location data from being used by anyone other than those directly involved in caring for people’s health—including protections from data being shared with police, other governmental agencies, employers, landlords, or educational institutions. With many public health departments already choosing to share data with first responders, including police, and with technology-based contact tracing apps creating avenues for a new form of surveillance, there is reason for concern that public health tools may be used to target activists.\textsuperscript{55} These concerns are a problem for public health for several reasons:

1. **Lack of privacy protections for contact tracing erodes trust in public health interventions.** Contact tracing relies on trust. The process only works if people are willing to self-report their contacts to health departments and/or if people are willing to use an app-based tool. One study found that a mobile app would require an adoption rate of approximately 60 percent of the population to control the pandemic,\textsuperscript{36} while another puts that number at 80 percent of smartphone users.\textsuperscript{37} However, countries that are using app-based contact tracing are seeing only about 20 percent of people download the apps.\textsuperscript{38} Without trust that one’s personal information will be protected and will not be used to criminalize them, the process will fail. It will also prevent people—particularly historically and structurally marginalized communities that have already experienced racism and discrimination at the hands of public health and police—from trusting health officials about proper protection from the virus.

2. **Helping police target activists, either intentionally or unintentionally, works against the interests of public health.** The field of public health, led by the American Public Health Association, is clear that police violence is a public health issue\textsuperscript{39} and that systemic racism both harms health and drives disproportionate policing of people of color. Activists across the country are calling for Black liberation and an end to racist, oppressive, deadly, and unhealthy systems used in policing and incarceration. A growing body of literature suggests that political activism, particularly the act of working toward something bigger than oneself and toward the welfare of one’s community, has a positive correlation with well-being.\textsuperscript{40} Putting tools meant to protect public health in the hands of police not only jeopardizes the work of health departments, but also discourages activism and increases the potential for harmful contact between police and activists. Some of the apps that tech companies have created have privacy protections in place that prevent even health departments from having identifiable information
on individuals. While this anonymity provides an added layer of protection from data being passed to police, the systems of surveillance that police are already using can still be paired with contact tracing technology to target activists and do more harm.

3. **Ill-considered data collection methods could lead to inaccurate contact tracing data, which could contribute to the misallocation of health-promoting resources and continued spread of COVID-19.** For example, if the public does not trust those collecting the data, including the tech companies managing digital contact tracing, they may be unlikely to voluntarily participate in contact tracing efforts. Distrust will justifiably be concentrated among people who have been historically and currently targeted by surveillance and policing, who are the same people experiencing the highest rates of COVID-19 infection. Further, one in five people do not own a smartphone, creating a problem for app-based contact tracing. Likely, this will skew the data by leaving out older people and people with low incomes—two populations particularly at risk of contracting COVID-19. With inaccurate data, funds and effort may be wasted by failing to address the needs of the community, resulting in prolonged inability to contain the spread of the virus.

4. **“History teaches that privacy invasions often outlive the emergency they are intended to combat.”** As public health departments set up these surveillance systems for the duration of COVID-19, they need to be careful not to create systems that will increase surveillance beyond the point where it is needed to protect the public health. Though Google and Apple have pledged that they will shut down their app platform once the pandemic is over, there is no clear timeline for when that will be—or how an “end” will be defined. Previous surveillance policies instituted in the US supposedly in response to acute crises and moments in history—like the Patriot Act, whose provisions were supposed to end in 2005—still continue to target communities of color.

**Considerations to Protect Both Privacy and Health**

Contact tracing—digital or manual—is an important tool to control the spread of COVID-19. Though there are privacy concerns, appropriate protections can ensure the tool is useful without perpetuating harm. As described earlier, there is historical precedent, case law, and model legislation that guide public health emergency response while protecting civil liberties. Such a response requires a commitment to the principles and practices of belonging, as defined by the Othering & Belonging Institute:

Belonging means more than just being seen. Belonging entails having a meaningful voice and the opportunity to participate in
the design of social and cultural structures; it means having the right to contribute to, and make demands on, society and political institutions. Belonging is more than just feeling included; it means that your well-being is considered and your ability to design and give meaning to its structures and institutions is realized.65

Many privacy advocates,66 antipolicing organizers,67 public health professionals,68 and activists have put forward principles to ensure that contact tracing data remain secure and in service of the public’s health. Some of those considerations for state and local governments, including state and local health departments, are:

1. First, center racial justice as a core principle of contact tracing, from recruitment, compensation, and training of staff, through program design and evaluation.

2. Then, ensure the contact tracing process is shaped and led by the community, particularly by historically and structurally marginalized members of the community, in partnership with community-based organizations and those most vulnerable to and most affected by COVID-19, including people of color, elders and seniors, people experiencing houselessness, people with disabilities, immigrants, and low-wage workers.

One successful example is a contact tracing partnership of the Public Health Institute (PHI) with the community in Clark County, Washington. Guided by principles of racial justice and health equity, PHI focused their recruitment of contact tracers on those who had experience working with the communities of Clark County that were most disproportionately impacted by COVID-19. Over 90 percent of the tracers hired were bilingual or multilingual and all were residents of Clark County. At the time the partnership began, Clark County was facing one of the largest COVID-19 clusters in the Northwest at Firestone Pacific Foods frozen fruit packing facility. Seventy-nine employees tested positive for COVID-19, but within one week, PHI was able to reach 85 percent of employees who had contact with positive cases and stop the spread of COVID-19 within the facility.69

3. As data are collected, prohibit public health departments from sharing identifying information and location data with any other agency or organization, including tech companies; employers; housing providers; educational institutions; and federal, state, and local law enforcement agencies, even if subpoenaed.

4. Delete all data as soon as it is no longer needed (e.g., as recommended by data security experts at MIT, after thirty days)10 to prevent surveillance from being extended beyond the time of the community spread of COVID-19, at which point contact tracing can be phased out as a tool for pandemic management. If digital contact tracing is being used, data
should be automatically deleted after thirty days or individuals should have control over manually deleting their own data at any point.

As we face the ongoing pandemic and uprisings against police violence, it is necessary to protect both public health and individual privacy. In fact, protecting individual privacy is a prerequisite for supporting public health. While privacy is valuable in its own right insofar as it is connected to human dignity, there are also very practical ways in which privacy promotes health. Ensuring that privacy can promote trust in the relationship between physicians and their patients is necessary for quality care. There is also research that documents the benefits of privacy for interpersonal relationships by allowing individuals the autonomy to decide who to share information with and when. Finally, societal benefits of protecting privacy include better quality health data for research and care, because people can trust that their private information will be protected. Though new surveillance technology provides a less labor-intensive option to track data, there is a great deal of risk that the data can be used for purposes that could fundamentally inhibit belonging and harm public health. By ensuring that COVID-19 data remain only within state and local health departments and are not shared with any other agency or company, public health officials can build trust and power with communities to ensure that the virus is traced accurately and safely.
Endnotes


15 CDC, “Contact Tracing: Frequently Asked Questions.”


21 Legal Information Institute, “Henning Jacobson.”


25 Walzer Leavitt, “Public Resistance or Cooperation?”


33 Albert Fox Cahn and John Yany Veiszlemein, “Beware: Bluetooth Ahead. The Civil Rights & Privacy Dangers of Deploying Bluetooth to


42 Fox Cahn and Yany Veiszlemlein, “Beware: Bluetooth Ahead.”

43 Cahn and Veiszlemlein, “Beware: Bluetooth Ahead.”


46 Jay Stanley and Jennifer Stisa Granick, “The Limits of Location Tracking in an Epidemic,” American Civil Liberties Union, April 8, 2020, 9.


52 Nass et al., *The Value and Importance of Health Information Privacy*.

53 Nass et al., *The Value and Importance of Health Information Privacy*. 