# Privacy and Pandemics

**Clarisa Long, Max Mendel Shaye Professor of Intellectual Property Law, Columbia Law School;**
**Editor, Genetic Testing and the Use of Information**

The current COVID-19 pandemic has created an unprecedented opportunity for governments to justify post-pandemic expansion of their surveillance and collection of data on citizens and noncitizens alike. The data collected could take multiple forms, but I will focus on two specific types of data collection.

The first is governmental mass collection of nonanonymized cell phone location data showing the physical location of people in a community without the consent of the surveilled, who are not suspected of any crime. The second is state-collected nonanonymized data on people's health or immunity status. Both of these raise fundamental information privacy and health privacy concerns. Both would require amendments of existing laws and regulations, or passage of sweeping new laws, in order to pass legal muster. Post-pandemic, governments may try to do exactly this.

In the information privacy community the relevant unit of data is "personally identifiable information," or PII.[1] In the health context, the relevant unit of data is called "protected health information," or PHI.[2] In times of national or global emergency, such as a pandemic, governmental collection of PII or PHI that in normal times would be either prohibited by law or questionable under social norms may become normalized and desirable to combat the spread of disease.

[1] See Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011) (stating that "PII is one of the most central concepts in privacy regulation. It defines the scope and boundaries of a large range of privacy statutes and regulations.").

[2] See HIPAA Guidelines, 45 C.F.R. § 160.103 ("*Protected health information* means individually identifiable health information.") (emphasis in original).

**In times of pandemic, extensive data collection, either of individuals' physical location or health status, may be desirable from a public health perspective.**

Evidence is emerging that countries that tested for COVID-19 early and monitored the movements of their citizens had better outcomes, both as to infection rates and as to death rates, than countries like the U.S. that did not engage in early testing and monitoring. In the *New York Times*, Anna Sauerbrey says, "Early and persistent testing helps. And so does tracking people."[3] *The Atlantic* magazine argues, "More transmissible and fatal than seasonal influenza, the new coronavirus is also stealthier, spreading from one host to another for several days before triggering obvious symptoms. To contain such a pathogen, nations must develop a test and use it to identify infected people, isolate them, and trace those they've had contact with. That is what South Korea, Singapore, and Hong Kong did to tremendous effect. It is what the United States did not."[4]

**Governments around the world are collecting location and tracking data on people in order to stem the spread of COVID-19.**

Contact tracing of infected individuals can be done by using cellphone location data. For example, government agencies in South Korea used "surveillance-camera footage, smartphone location data and credit card purchase records to help trace the recent movements of coronavirus patients and establish virus transmission chains," according to the New York Times, whereas Israel is looking to use previously-collected cell phone location data[5] to attempt contact

[3] Anna Sauerbrey, "Germany Has Relatively Few Deaths From Coronavirus. Why?," New York Times, March 28, 2020, available at https://www.nytimes.com/2020/03/28/opinion/germany-coronavirus.html (arguing that aggressive early testing and tracking individuals' locations was responsible for the relatively death rate from COVID-19 infection in Germany).

[4] Ed Yong, How the Pandemic Will End, The Atlantic (March 25, 2020), available at https://www.theatlantic.com/health/archive/2020/03/how-will-coronavirus-end/608719/.

[5] See David M. Halbfinger, Isabel Kershner & Ronen Bergman, "To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data," New York Times, March 16, 2020, available at https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html.

tracing of individuals potentially infected with COVID-19.[6] Local governmental authorities in Italy are reported to be using citizens cellphone location data to analyze the degree of compliance with official lockdown orders.[7] The government of Delhi has started tracking cellphone location data of people who are thought to be infected with COVID-19 and who have been quarantined at home.[8] More governments may choose to do the same.

In the U.S., Google -- a private sector entity, not the government -- says it will be publishing cell phone location data, but this data is not tied to any one single person. According to CNN, Google has "said the findings are 'created with aggregated, anonymized sets of data from users who have turned on the location history setting, which is off by default' in Google's services."[9]

Such monitoring and tracking of individuals' movements, especially in the early stage of a pandemic, can be effective, even dramatically effective in slowing the spread of the virus. It is even more effective and can be targeted when nonanonymized. In such public health emergencies, data collection of PII can have enormous social benefits. But under existing U.S. law, however, the U.S. Supreme Court has ruled that *nonanonymized* collection of cell phone location data by governmental entities is a search protected by the Fourth Amendment of the U.S. Constitution, and as such, requires a warrant supported by probable cause.[10]

---

[6] Ed Yong, How the Pandemic Will End, The Atlantic (March 25, 2020), available at https://www.theatlantic.com/health/archive/2020/03/how-will-coronavirus-end/608719/.

[7] Id. (citing https://milano.corriere.it/notizie/cronaca/20_marzo_17/coronavirus-gallera-in-lombardia-1640-decessi- 16620-positivi-e3875744-686d-11ea-9725-c592292e4a85.shtml?refresh_ce-cp).

[8] See Swati Gupta, "At Least One Indian Territory is Tracking the Phones of Suspected Coronavirus Patients," CNN, April 1, 2020, available at https://us.cnn.com/world/live-news/coronavirus-pandemic-04-01-20-intl/index. html (quoting Delhi chief minister Arvind Kejriwal as saying "We have made a decision and with help from the police, people who have been asked to quarantine themselves at home, we will track their phones over the past few days to ensure that they were staying at home.").

[9] Amy Woodyatt, Google to release your location data to help fight coronavirus pandemic, CNN Business, April 3, 2020, available at https://www.cnn.com/2020/04/03/tech/coronavirus-google-data-sharing-intl-scli/index.html.

[10] See Carpenter v. U.S., 138 S. Ct. 2206 (2018) (holding that "The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

In the lengthy and usually-unread terms of service that cell phone customers have to sign, cell phone users give wireless companies the ability to collect and sell their location data.[11] Private sector firms that currently collect cell phone location data generally take the position that the data are anonymized,[12] although some privacy experts believe that even anonymized cellphone location data, because it is often collected with a high degree of granularity, can be used to identify individuals.[13] But app creators could write clauses into their Terms of Service saying that users consent to their nonanonymized cell location data being shared with federal and state authorities, law enforcement or otherwise, in the absence of a warrant. (The degree to which clauses that require individuals to consent in advance to waive their Fourth Amendment rights, in exchange for receiving cellphone services, are themselves enforceable is another matter.)

**Once surveillance and data collection mechanisms become established, however, they could become permanent.**

The threats to information privacy, whether in the collection of nonanonymized cellphone location data or of health status, arise after the pandemic is over. Once the mechanisms to gather and use PII and PHI have been established to meet a public health emergency, they may well prove difficult if not impossible to dismantle. And governments face every temptation to leave surveillance protocols in place. History teaches us that once established, governmental powers of surveillance of, and data collection on, its citizens and residents is unlikely to be voluntarily scaled back.[14] And history has also taught us that once data is collected for one purpose it is difficult to prevent it from being used for other unrelated purposes.

---

[11] Shannon Liao, "New York City Might Ban Wireless Companies From Selling Your Location Data," CNN Business, July 24, 2019, available at https://www.cnn.com/2019/07/24/tech/nyc-cellphone-location-data-sale-ban/index.html.

[12] See, e.g., Donie O'Sullivan, "How the Cell Phones of Spring Breakers Who Flouted Coronavirus Warnings Were Tracked," CNN, April 4, 2020, available at https://www.cnn.com/2020/04/04/tech/location-tracking-florida-coronavirus/index.html.

[13] See, e.g., Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller & Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," New York Times, Dec. 10, 2018, available at https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[14] See, e.g., the Foreign Intelligence Surveillance Act Amendments of 2008, 50 U.S.C. § 1881-81g (2020), which have been extended several times since their creation, despite "sunset" provisions written into the legislation.

**In addition to collecting PII in the form of cell phone location data, governments might also collect PHI in the form of COVID-19 test results or immunity results.**

An idea that is increasingly gaining traction, both in the U.S. and elsewhere, is that of creating a nonanonymized database of names of individuals who have recovered from the virus and are thus presumably immune. Dr. Anthony Fauci, the Director of the National Institute of Allergy and Infectious Diseases (NIAID) at the National Institute of Health and the U.S. government's top infectious-disease official, has said he believes that such "conferred immunity" protects against reinfection.[15]

Germany, for example, is contemplating a proposal to issue "immunity certificates" that would allow individuals who had tested positive for antibodies to the virus to leave lockdown.[16] According to the German newspaper Der Spiegel,[17] researchers at the Helmholtz Centre for Infection Research in Braunschweig, Germany "want to send out hundreds of thousands of antibody tests over the coming weeks that could allow people to break free of the lockdowns."[18] Italy is reported to be considering a similar strategy.[19]

For such health care measures to work and to avoid fraud, however, governmental authorities would need to keep a database, similar to driver's license databases, on who holds an immunity

---

[15] See Joshua M. Epstein, Are We Already Missing the Next Epidemic?, Politico Magazine, March 31, 2020, available at https://www.politico.com/news/magazine/2020/03/31/coronavirus-americafear-contagion-can-we-handle-it-157711.

[16] See Daniel Wighton & David Chazan, "Germany Will Issue Coronavirus Antibody Certificates to Allow Quarantined to Re-Enter Society: Researchers to Test Thousands for Immunity As Berlin Plans Exit Strategy for Pandemic Lock Down," The Telegraph, March 29, 2020, available at https://www.telegraph.co.uk/news/2020/03/29/ germany-will-issue-coronavirus-antibody-certificates-allow-quarantined/.

[17] See Sauerbrey, note 3 supra.

[18] See Adam Bienkov, "Germany Could Issue Thousands of People Coronavirus 'Immunity Certificates' So They Can Leave the Lockdown Early," Business Insider (March 30, 2020), available at https://www.businessinsider.com/coronavirus-germany-covid-19-immunity-certificates-testing-social-distancing-lockdown-2020-3.

[19] See Jason Horowitz, "In Italy, Going Back to Work May Depend on Having the Right Antibodies, New York Times," April 4, 2020, available at https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html?action=click&module=Top%20Stories&pgtype=Homepage.

certificate and who does not. That means collecting and recording, in *non-anonymized form*, the PHI of individuals and their antibody status regarding COVID-19. This is necessary in order to minimize the opportunity for fraud by people eager to return to work. (Another concern that has been raised surrounding immunity certificates is "whether people might deliberately seek to get infected in order to -- hopefully -- recover and go back to work," which could undermine the flattening of the infection curve that governments and health experts are trying to achieve by requiring social distancing.[20]) And such a database would provide a juicy target for hackers and trolls.

Immunity databases in times of pandemic -- and even post-pandemic -- could provide public health officials with a powerful tool to fine-tune quarantine efforts. Large scale quarantines can be disastrous for the economy even as they are necessary from a public health perspective. Premature lifting of quarantines and stay-at-home orders could allow COVID-19 to return with a vengeance. Yet at the same time, the longer people are out of work and non-essential businesses are shut down, the harder it will be for them to recover financially and for the economy to turn around. Allowing people who have obtained immunity to COVID-19 to return to work would allow economies around the world to recover faster, and at least as importantly, would allow individuals to regain their own financial equilibria.

**This raises important issues and challenges to information privacy and health privacy law.**

Post-pandemic, how can federal, state, and local governments thread the needle of mounting effective and timely responses to a fast-moving public health crisis, while simultaneously protecting (or at least not worsening) existing legal protection for PHI? Existing state-level models may provide a template for further exploration.

[20] Laura Smith-Spark, "Is an 'Immunity Certificate' the Way to Get Out of Coronavirus Lockdown?," CNN, April 3, 2020, available at https://www.cnn.com/2020/04/03/health/immunity-passport-coronavirus-lockdown-intl/index.html.

Several states have laws requiring medical professionals to provide health risk information to potentially affected individuals through contact tracing.[21] For instance, New York State's HIV Reporting and Partner Notification law (HIVRPN) law allows for contact tracing of cases of AIDS, HIV related illness or HIV infection.[22] It requires that "[d]octors and labs must report to the Health Department the names of persons with HIV infection, HIV illness and AIDS" and "must also report the names of sex and needle-sharing partners of people who test HIV positive that are known to the doctor."[23] The HIVRPN has been described as "one of the most aggressive statutes to protect the public . . . [o]n a spectrum that puts individual patient confidentiality on one end and public health protection on the other."[24] Although not without controversy, the HIVRPN has been lauded in the affected communities as a public health success,[25] and the New York State Department of Health takes the information privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) into account when enforcing state public health laws.[26]

Post-pandemic, one key issue that must be addressed head on, should governmental database(s) of immunity status be created at the federal or state level, is obtaining informed consent from each of the individuals in such a database to share their nonanonymized testing results with state authorities. This might seem like a no-brainer -- who would not mind the state knowing their antibody status if it meant they could return to work earlier and be released from stay-at-home

---

[21] See, e.g., N.Y. Pub. Health Law § 2130: Communicable diseases; control of dangerous and careless patients; commitment.

[22] See N.Y. Pub Health § 2133: Contact tracing of cases of AIDS, HIV related illness or HIV infection.

[23] N.Y. State: Dep't of Pub. Health, What Is Partner Notification?, available at https://www.health.ny.gov/ diseases/ aids/providers/regulations/reporting_and_notification/about_the_law.htm#quest2 (stating that "[d]octors and labs must report to the Health Department the names of persons with HIV infection, HIV illness and AIDS" and "must also report the names of sex and needle-sharing partners of people who test HIV positive that are known to the doctor").

[24] Jacquelyn Burke, Discretion to Warn: Balancing Privacy Rights with the Need to Warn Unaware Partners of Likely HIV/AIDS Exposure, 35 B.C. J.L. & Soc. Just. 89, 105 (2015).

[25] See N.Y. State Dep't of Health Aids Inst., The Impact Of New York's HIV Reporting And Partner Notification (Hivrpn) Law: General Findings Report 5 (2006), available at https://www.health.ny.gov/diseases/aids/providers/ regulations/reporting_and_notification/docs/impactreport.pdf (showing that "[a] study of 132 partners of HIV-positive individuals located through health department notification found that 87% thought the Health Department did the right thing in telling them about their exposure, and 92% thought that the Health Department should continue to notify persons exposed to HIV.").

[26] See Office of Mental Health, New York State, "Information for Consumers: Privacy Rule," available at https://omh.ny.gov/omhweb/hipaa/consumers/privacy/.

orders? -- but the underlying issues and implications are not so simple. Given how little the scientific community knows about COVID-19, it is not clear that even a positive test for antibodies is a guarantee of immunity. Similarly, false positive tests -- in which a person inaccurately tests positive for the antibody, and therefore appears immune when in fact they are not -- could undermine the effectiveness of an immunity database. And because all viruses mutate, individuals' immunity status would have to be updated periodically as the virus mutates over time, so reporting immunity status would likely not be a one-time event.

Like HIV, COVID-19 is a transmissible virus that can be readily diagnosed, and for which early detection and treatment are clearly beneficial. Because immunity, whether from vaccination or from successful recovering from a COVID-19 infection, would be viewed as a desirable status, this does not present some of the concerns of social or economic discrimination that a database of results like HIV-positive status present. Even so, such a database of non-anonymized PHI, available to an array of government actors, represent a departure from existing laws and norms regarding the treatment of PHI.

The least controversial route, from a privacy perspective, would be to create a voluntary opt-in government database of people with immunity status, with no penalties for declining to opt in. But as a public health response to monitoring seropositive status after the current pandemic, voluntary self-reporting of non-anonymized immunity status would be only a partial solution. Public health responses that rely on voluntary cooperation of mass numbers of people, some of whom may not have cellphones or even internet access, will not be as effective as mass mandatory self-reporting.[27]

Legal rules and social norms regarding state collection of nonanonymized PHI might not necessarily stop with COVID-19. COVID-19 is not the only transmissible virus. The slope from non-anonymized COVID-19 immunity databases, to governmental collection of non-anonymized

[27] The Associated Press, School Shutdowns Raise Stakes of Digital Divide for Students, New York Times, March 30, 2020, available at https://www.nytimes.com/aponline/2020/03/30/us/ap-us-virus-outbreak-digital-divide.html.

information about individuals' immunity status to other viruses, then to their vaccination records, then to their public health wellness generally, is a slippery one indeed.

**These issues will not be going away.**

There will always be a next pandemic at some point in the future, if not of COVID-19 then of some other infectious agent. The challenges that pandemics present to information privacy are not going to go away or lessen any time soon. After the current pandemic is over, lawmakers, public health experts, and information privacy advocates need to address these issues and balance privacy protection with public health concerns so that the U.S. can be better prepared for the next pandemic, whenever it may come.