PART II: RESPONSE ISSUES

Good Health and Good Privacy Go Hand-in-Hand

Jennifer Daskal*

In the United States, numerous pundits and commentators noted the similarities between the 9/11 attacks and the health pandemic caused by COVID-19.[1] Both shook the nation, exposing deep vulnerabilities to external forces. Both caused large numbers of casualties, albeit on different orders of magnitude.[2] And

* Professor and Faculty Director, American University, Washington College of Law. Special thanks to Laura Denardis, Gene Fidell, Alex Joel, Matt Perault, Lindsay Wiley, and Alan Rozenshtein for helpful conversations and input. A special thanks as well to my wonderful research assistant Daniel de Zayas.

1. *See, e.g.*, Alex Joel, *9/11 All Over Again*, JUST SECURITY (Apr. 10, 2020), https://perma.cc/VY29-8YXS (suggesting how lessons learned from 9/11 could be applied in the response to COVID-19); Peter Swire, *Security, Privacy and the Coronavirus: Lessons from 9/11*, LAWFARE (Mar. 24, 2020, 2:46 PM), https://perma.cc/YD6Y-UYTV (same); Nick Paton Walsh, *9/11 Saw Much of Our Privacy Swept Aside. Coronavirus Could End It Altogether*, CNN (May 16, 2020, 1:27 PM), https://perma.cc/T4VM-MFFM (quoting Edin Omanovic, Advocacy Director, Privacy International: "The surveillance industry 'understands that this is an opportunity comparable to 9/11 in terms of legitimizing and normalizing surveillance.'").

2. Michael Finnegan, *New York State's Coronavirus Deaths Now More Than Double 9/11 Fatalities*, L.A. TIMES (Apr. 8, 2020), https://perma.cc/DH7D-NSXA (marking the point in time at which the

both resulted in significant restrictions on civil liberties, justified as needed to protect the nation, including wide-ranging calls for a surge in surveillance to protect against would-be terrorists and pathogens, respectively.

But there was and is a key difference. After the 2001 attacks, the U.S. government ramped up its tracking tools in order to identify and stop would-be terrorists, much of which was done clandestinely. Even when the programs were disclosed and, in some cases, transformed into congressionally-approved systems of surveillance, key operational details, including the identities of those being tracked, remained and remain secret.[3] The entire system depends, in large part, on nondisclosure in order to be effective. It would, after all, largely defeat the purpose if suspects knew how and when they were being tracked.

Health surveillance in response to a pandemic, however, has a very different goal. The primary purpose is to educate and inform—to let people know where there are large numbers of people congregating so that they can take steps to avoid what might become the next disease hot spot; to tell individuals that they have been in close contact with someone deemed contagious; to make visible and transparent the need to test and self-quarantine; to let those subject to quarantine orders know that their movements are being monitored in order to induce compliance. The more transparent and open—or, depending on one's perspective, the more panopticon-like—the more effective.[4]

This has led to a remarkable amount of clarity, as well as an open and robust debate, about the kinds of surveillance employed or considered in support of better health outcomes; how best to design the surveillance systems that are being employed; whether, when, and in what cases use of surveillance systems should

---

number of COVID-19 deaths exceeded that of deaths from the 9/11 attacks). Since then, numbers of COVID-19 deaths have continued to climb. JOHNS HOPKINS UNIVERSITY, COVID-19 UNITED STATES CASES BY COUNTY, https://perma.cc/TLL3-CFHM.

3. *Compare* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N.Y. TIMES (Dec. 16, 2005), https://perma.cc/KLT6-CH3F (revealing the existence of the Terrorist Surveillance Program authorized by President George W. Bush that, without FISA oversight, allowed NSA interception of the content of international communications to or from the United States when a communicant was suspected of being linked to al Qaeda or a related terrorist organization), *with* FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (amending the Foreign Intelligence Surveillance Act of 1978 to, in essence, authorize the warrantless collection of foreigners' communications, subject to programmatic approval by the Foreign Intelligence Surveillance Court). Another example is that of the telephone metadata, revealed by the Snowden leaks, transformed under the USA Freedom Act. Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified at 50 U.S.C. §1861). Details, however, of who was targeted under that program were classified. *See generally* David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SECURITY L. & POL'Y 377 (2016) (providing a comprehensive charting of past and future sea changes in foreign intelligence surveillance).

4. There are of course some exceptions to this. Secrecy can help support a goal of compliance with mandatory quarantines, for example, in the wake of concerns about people bypassing or manipulating an applicable surveillance scheme. And there remains a use for Intelligence community tracking of things like extraterritorial disease spread—as was reportedly done by the Intelligence community in 2019, as it tracked the disease spread in China, thereby providing an early warning system. *See* Josh Margolin & James Gordon Meek, *Intelligence Report Warned of Coronavirus Crisis as Early as November: Sources*, ABC NEWS (Apr. 8, 2020, 9:55 PM), https://perma.cc/4M5T-2LHD. In general, however, health surveillance works via public engagement and public disclosure.

be universal versus targeted; and, relatedly, whether, when, and in what cases they should be mandated versus consent-based.

This short article seeks to contribute to that discussion, arguing that whereas many presume that surveillance and privacy work in tension, that need not and should not be the case. To the contrary, good health surveillance and good privacy should be treated as mutually reinforcing goals. This article makes this case in three parts. Part I sets the scene, categorizing various types of surveillance schemes that have or likely will be considered, with a particular focus on the United States, but a nod to what some other countries are doing as well. It is not meant to be exhaustive, but to provide broad categories to guide the discussion in Part II. Part II presumes governmental mandates—something that to date has been the exception rather than the rule in the United States, at least when it comes to governmental, as opposed to employer-mandated action.[5] It nonetheless reflects an approach that public health authorities may push for in the future, and thus identifies and addresses the constitutional and statutory considerations applicable to each. And Part III provides the core policy considerations, describing how and why to design systems in which good privacy is treated as a key component of good health.

I. HEALTH SURVEILLANCE: DEFINING THE CATEGORIES

For many, the word "surveillance" evokes images of Orwellian Thought Police engaged in constant monitoring and control of not just action but thought.[6] Health surveillance, though, is something very different—referring to the tracking of disease patterns and health status in a systematic and ongoing way in order to, among other core goals, minimize disease spread.[7] When public health experts talk about surveillance, its connotation is almost entirely positive—about promoting good health and preventing disease spread. Widespread symptom and disease reporting, for example, helps identify emergent epidemics, track disease spread, and better allocate resources and treatment in response. Other forms of health surveillance applicable to the current pandemic involve what has often been called contact tracing—to identify those whom a sick person has been in contact with and are therefore at risk of becoming ill as well.

But while the primary focus of health surveillance is on the disease, with a goal of identifying and minimizing disease spread, diseases are of course carried and

5. Brian Heater, *Can Employers Mandate COVID-19 Testing?*, TECHCRUNCH (Apr. 20, 2020, 3:46 PM), https://perma.cc/4E4T-PW2G; *see also* Dave Gershgorn, *We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World*, ONEZERO (Apr. 9, 2020), https://perma.cc/F379-HETV (discussing what other countries are doing around the world regarding COVID-19 surveillance).

6. *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR: A NOVEL (1949).

7. *See, e.g.*, Richard C. Dicker, *A Brief Review of the Basic Principles of Epidemiology*, *in* FIELD EPIDEMIOLOGY 20-21 (Michael Gregg ed., Oxford Univ. Press 3d ed. 2008) (defining public health surveillance as "the ongoing, systematic collection, analysis, and interpretation of [health-related] data essential to planning, implementation, and evaluation of public health practice, closely integrated with the dissemination of that data to those who need to know").

transmitted by people. Hence disease tracking and people tracking almost inherently overlap. This article focuses on those areas of overlap. It starts by categorizing, in a concededly broad-brushed way, the different kinds of health surveillance being employed or considered, and assessing the privacy considerations raised by each. These categories frame the legal and policy discussion in Part II.

A. Aggregate Level Analysis

Aggregate level analysis involves the use of data sets to predict population-level trends, without identifying or linking the data to particular individuals. Kinsa, for example, used real-time temperature data collected from its smart thermometer to forecast the next COVID-19 hot spots—something it had done previously to predict flare-ups of the seasonal flu.[8] The analysis employs data from users who have opted in to share anonymous temperature readings and other symptoms.[9] Location analysis company Cuebiq estimated the relative mobility of people over time, using a representative sample of about 15 million smartphone users nationwide.[10] Facebook, Google, and Apple each rolled out mapping efforts that use aggregated data to provide information about things like where people are congregating.[11] This kind of location data and aggregate mapping provide useful information for officials seeking to minimize congestion in particular areas and for anyone seeking to avoid crowds.[12]

These are just some examples of many. This kind of surveillance uses sensitive location and health data, but in an aggregated and de-identified form—in order to reveal trends rather than track or reveal information about particular, individualized users. Even this kind of analysis poses privacy risks, depending on how it is presented. If the information made public is sufficiently granular and detailed—such as mobility data on very small population sets or temperature data combined with detailed location information—the analysis could be used to pinpoint particular individuals and thereby map their movement and health. But so long as the data set is sufficiently large and aggregated with key protective measures put in place, the privacy risks are low.[13]

---

8. Ruth Reader, *This Map Uses Smart Thermometers to Detect Potential Surges in COVID-19 Cases*, FAST CO. (Mar. 20, 2020), https://perma.cc/KZ6W-B99H.

9. Kinsa Data Team, *The Demographics Behind Kinsa Insights and the US Health Weather Map* (Apr. 4, 2020), https://perma.cc/9K9Q-5HWG. The company also commits not to sell personally identifying information or individual data. KINSA, KINSA'S PRIVACY PRINCIPLE, https://perma.cc/32SL-8PES.

10. Gabriel J.X. Dance & Lazaro Gamio, *As Coronavirus Restrictions Lift, Millions in U.S. Are Leaving Home Again*, N.Y. TIMES (May 13, 2020), https://perma.cc/VZ23-L9RX.

11. *Apple Makes Mobility Data Available to Aid COVID-19 Efforts*, APPLE NEWSROOM (Apr. 14, 2020), https://perma.cc/9KYE-S7FX; Taylor Hatmaker, *Facebook Launches COVID-19 Data Maps for the US, Will Take Its Symptom Tracking Efforts Global*, TECHCRUNCH (Apr. 20, 2020, 12:15 PM), https://perma.cc/8RSW-GND2.

12. NURIA OLIVER ET AL., MOBILE PHONE DATA AND COVID-19: MISSING AN OPPORTUNITY? (2020), https://perma.cc/H84Y-W3ST; Jen Fitzpatrick & Karen DeSalvo, *Helping Public Health Officials Combat COVID-19*, GOOGLE (Apr. 3, 2020), https://perma.cc/K4M7-WY87.

13. *Enlisting Big Data in the Fight Against Coronavirus: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 116th Cong. 2 (2020) (statement of Prof. Ryan Calo) [hereinafter *Hearing*

Notably, these examples involve companies analyzing user data already in their possession, and only sharing the final, aggregated analysis. Alternatively, underlying data sets might be shared with outsiders, whether researchers or government officials, so as to allow those outsiders to engage in their own analysis. This enables the combination of combine multiple different data streams, which creates additional privacy risks. As several studies have demonstrated, it is nearly impossible to anonymize personal data in ways that fully protect against re-identification.[14] Several advocates and others have raised concerns about Facebook's sharing of aggregate location data with researchers on these grounds; these concerns apply to sharing by other companies as well.[15] That said, the use of technical tools, including differential privacy techniques, and other privacy protective policies and practices can minimize, albeit not fully eliminate, these risks.[16]

B. Individual Level Analysis

The privacy concerns ratchet up significantly once surveillance schemes shift from aggregate-level analysis to individual-level tracking and tracing. The following describes three different kinds of individual-level surveillance, identifying some key considerations applicable to each.

1. Contact-Tracing

Contact tracing is something that just about every public health official recommends as part of a broader program of test, trace, treat, and isolate.[17] It works by identifying someone who has the virus, ideally confirmed via testing. The close contacts of the person who has the virus are identified and notified so that they can themselves self-isolate and, ideally, get tested as well. This minimizes the chance of

---

Statement] (noting that when data are aggregated and displayed only as a relative percentage, the risks to individuals are mitigated).

14. Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCI. 536 (2015) (reidentifying 90 percent of the credit card records of 1.1 million people using only four spatiotemporal points); Luc Rocher et al., *Estimating the Success of Re-Identification in Incomplete Datasets Using Generative Models*, 10 NATURE COMMS. 1 (2019), https://perma.cc/4SVL-8ZKH (concluding that 99.98% of American could be correctly re-identified using 15 demographic attributes); C. Christine Porter, *De-identified Data and Third Party Data Mining: The Risk of Re-identification of Personal Information*, 5 SHIDLER J.L. COM. & TECH. 3, 5 (2008) (chronicling early research of and efforts to re-identify anonymized data); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (providing comprehensive scrutiny of anonymization and re-identification).

15. *See, e.g.*, Issie Lapowsky, *Facebook Data Can Help Measure Social Distancing in California*, PROTOCOL (Mar. 17, 2020), https://perma.cc/X23B-E6UN.

16. Gregory E. Simon et al., *Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care Records*, J. ELECTRONIC HEALTH DATA & METHODS 1, 3-7 (2019), https://perma.cc/6LLN-5GMM (identifying sources of re-identification risk for health research datasets and proposing a framework to mitigate such risk).

17. DANIELLE ALLEN ET AL., ROADMAP TO PANDEMIC RESILIENCE 12 (2020), https://perma.cc/9ADB-E27N [hereinafter ALLEN ET AL., ROADMAP TO PANDEMIC RESILIENCE]; CRYSTAL WATSON ET AL., A NATIONAL PLAN TO ENABLE COMPREHENSIVE COVID-19 CASE FINDING AND CONTACT TRACING IN THE US (2020), https://perma.cc/Z9QU-JX6Y [hereinafter WATSON ET AL., NATIONAL PLAN TO ENABLE COVID-19 CASE FINDING AND CONTACT TRACING].

further disease spread. Its usefulness relies, in large part, on access to sufficient testing. Tracing without testing is inherently less useful than tracing plus testing.

Historically, contact tracing has been done by humans, via case-by-case interviews and personal follow-up. A public health official interviews a person who is deemed sick to identify those with whom the sick person has been in contact. Those contacts are then notified via a call, text, email, or, if necessary, house visit—informing them of potential exposure and recommended next steps. A Johns Hopkins study estimates that the United States needs more than 100,000 tracers to effectively fill this role; as of April 2020, there were approximately 2,200.[18]

Memories, however, are invariably faulty. And even with perfect recall, a presumptively sick individual may not know the identity of, say, those they stood in line next to for 20 minutes or inadvertently squished against in a crowded subway car (assuming we ever get to the point of riding crowded subway cars again).

Enter digital tracing tools. They can, at least in theory, mitigate the problems of imperfect recall and incomplete information. But the means of doing so vary greatly, in ways that matter significantly to the analysis of both effectiveness and risk. The following describes three (of many) possible approaches.

a. Government Monitoring

This is the approach of South Korea. Once someone tests positive, the government—used a combination of mobile phone data, credit card information, and facial recognition software—to create a retrospective mapping of that person's movements.[19] Israel similarly repurposed cell-site location data previously collected for anti-terrorism purposes to identify—albeit, in a fairly imprecise way—those who have been physically near an infected individual.[20] Both countries then used this data to identify and notify those deemed to have been in proximity with those who fell ill.

South Korea has coupled this individual notification system with a public alert system as well. The government posts the past movements of sick individuals publicly on an anonymous basis. Others can then compare their own travel history with those of sick individuals to assess infection risk. Mapping also can highlight a particular locus of disease spread—if, for example, a significant number of sick people all spent time in the same location prior to falling ill.

This provides potentially useful information, but at high cost. While individuals are not named, the information provided—the public display of one's location history for a period of two weeks—is often sufficiently detailed to enable others

18. WATSON ET AL., NATIONAL PLAN TO ENABLE COVID-19 CASE FINDING AND CONTACT TRACING, *supra* note 17, at 8; Jessie Hellmann, *Why Contact Tracers Are Key to Unlocking Economy*, THE HILL (Apr. 18, 2020, 5:00 PM), https://perma.cc/KC6T-CPHG.

19. Natasha Singer & Chloe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, N.Y. TIMES (Mar. 23, 2020), https://perma.cc/4MSF-ZBDY (updated Apr. 17, 2020); Mark Zastrow, *South Korea Is Reporting Intimate Details of COVID-19 Cases: Has It Helped?*, NATURE (Mar. 18, 2020), https://perma.cc/XZ7S-D5C7.

20. David M. Halbfinger et al., *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*, N.Y. TIMES (Mar. 16, 2020), https://perma.cc/M6UX-S5KP (updated Mar. 18, 2020).

to identify not only who has been sick, but where they have gone every moment of every day. This results in the private disclosure of highly personal information and has, in numerous circumstances, led to harassment and shaming.[21]

b. Contract Tracing Apps

Multiple other countries have pushed contact tracing apps to be downloaded on smartphones by citizens and residents.[22] Such apps generally use either Bluetooth technology (which can be used to map proximity) or GPS (which maps location), or a combination of both, to identify when one user's phone is in proximity with another phone with a compatible app.[23] When one such app user tests positive, the data can be used to identify other app users with whom the sick person crossed paths. This can supplement the work of human contact tracers. And the notifications can be coupled with warnings and other demands, such as mandatory testing and isolation.

The technical and practical means of contact tracing storage vary across different apps. Key considerations axes include the type of data used and the means of collection and storage. Collection of Bluetooth data is generally considered less privacy intrusive than collection of GPS data, as it maps proximity without revealing location.[24] This is important: location data could be used to reveal whether one went to a prohibited bar, club, or other location, whereas Bluetooth data would reveal contacts without showing where those contacts were physically located. But Bluetooth data is not privacy risk-free; it can be combined with other data to infer location, even if location tracking is not itself turned on, and it can reveal a significant amount of information about contacts and associations over time.[25]

Centralized, governmental collection is also deemed more privacy invasive than decentralized storage systems.[26] In April 2020, for example, a group of 300

21. *Coronavirus Privacy: Are South Korea's Alerts Too Revealing?*, BBC (Mar. 5, 2020), https://perma.cc/6DP9-F8PM. (describing online harassment after a series of alerts about the whereabouts of those who tested positive for COVID-19). *See also* Min Joo Kim, *Tracing South Korea's Latest Virus Outbreak Shoves LGBTQ Community into Unwelcome Spotlight*, WASH. POST (May 11, 2020), https://perma.cc/26E9-7KE9.

22. *See, e.g.*, Natasha Lomas, *UK Gives Up on Centralized Contact Tracing Apps—Will "Likely" Switch to Model Backed by Apple and Google*, TECHCRUNCH (June 18, 2020, 10:39 AM), https://perma.cc/32UA-G4BA; Manish Singh, *India's Contact Tracing App Tops 100 Million Users in 41 Days*, TECHCRUNCH (May 12, 2020, 2:27 PM), https://perma.cc/FVY8-AHN6; Dean Koh, *Singapore Launches New App for Contact Tracing to Combat Spread of COVID-19*, MOBIHEALTHNEWS (Mar. 20, 2020, 10:38 AM), https://perma.cc/BW5Z-TQXF.

23. *See, e.g.*, Patrick Howell O'Neill, Tate Ryan-Mosley & Bobbie Johnson, *A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them*, MIT TECH. REV. (May 7, 2020), https://perma.cc/B7W3-4JNB (cataloguing different apps).

24. *See, e.g.*, Stacey Gray, *A Closer Look at Location Data: Privacy and Pandemics*, FUTURE OF PRIVACY F. (Mar. 25, 2020), https://perma.cc/YZC8-J83C.

25. *Id.*; *see also* Askan Soltani, Ryan Calo & Carl Bergstrom, *Contact Tracing Apps Are Not a Solution to the COVID-19 Crisis*, TECH STREAM (Apr. 20, 2020), https://perma.cc/SY4Q-PACU.

26. *See, e.g.*, Jennifer Daskal, *Digital Surveillance Can Help Bring the Pandemic Under Control—but also Threatens Privacy*, THE CONVERSATION (Apr. 9, 2020, 8:07 AM), https://perma.cc/95ND-Y9JL.

concerned scientists warned that centralized collection systems risked "mission creep" and misuse by malicious actors.[27] After all, such data would be of obvious interest to intelligence and law enforcement officials seeking to draw so-called social graphs, meaning a mapping of associations and locations of persons over time. In Australia, health authorities rebuffed requests by law enforcement to include in the Australian contract tracing apps added "capabilities" useful for law enforcement; Australian authorities later emphasized that the data were for "disease detectives" only.[28] Other law enforcement and intelligence authorities are likely to recognize the potential usefulness of such data and make demands as well. Such centralized databases risk becoming targets for foreign intelligence, would-be hackers, and other malicious actors.

In response to some of these concerns, an array of non-profits, tech companies, and universities have rolled out decentralized contact tracing systems, akin to the tracing systems just described, but using systems that store the relevant data on a user's phone, without sharing it with a government official or other centralized repository of such data. Notably, the widely discussed Apple-Google system, rolled out in May 2020, supports this kind of decentralized approach. It operates on an opt-in basis and, at least according to the promises made, employs Bluetooth technology only.[29] The relevant data are stored exclusively on an individual user's phone. The government does not collect the relevant data, absent a decision by a user to self-report. Once someone self-identifies as sick, the system sends alerts to the other users with whom the sick person's phone has been in contact, without employing any centralized database. Apple and Google assert that relevant data will be deleted once they is no longer useful—presumably 14 to 21 days for contact tracing purposes.

From a privacy perspective, this has the advantage of decentralization—meaning that there is no government central database to serve as a lure for hackers. There is also less risk that data collected for health purposes will then be employed for other purposes, leading to the kind of "unprecedented surveillance

27. Joint Statement from Scientists and Researchers on Contact Tracing (Apr. 19, 2020), https://perma.cc/LMY9-ZJHL.

28. Paul Karp, *Government Refuses Police Request for Access to Australian Coronavirus Contact Tracing App*, GUARDIAN (Apr. 23, 2020, 4:02 PM), https://perma.cc/LQ7M-M9YZ; Dr. Nick Coatsworth, Deputy Chief Med. Officer, Press Conference about Coronavirus (COVID-19) (Apr. 23, 2020), https://perma.cc/5A22-XGRD.

29. The system supports the collection of proximity as opposed to location data—allowing for background, continuous use of Bluetooth technology that can be used in connection with compatible contact tracing apps. If two users with compatible apps come within sufficient proximity of each other, they then exchange unique, and regularly updated, codes that serve as tracking numbers. *See* Apple-Google, *Exposure Notification: Frequently Asked Questions* (May 2020), https://perma.cc/5PSK-7V9S. Reporting has revealed that the Google system only works—given the design of Android phones—when *both* location services (meaning GPS tracking) and Bluetooth capabilities are turned on. This has led some to warn that Google could continue to collect location data from app users in ways that violate promises made. Google, for its part, maintains that, even if location services are turned on, the relevant apps do not collect that data. *See* Natasha Singer, *Google Promises Privacy With Virus App but Can Still Collect Location Data*, N.Y. TIMES (July 20, 2020), https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html.

of society at large" that many fear.[30] However, there are trade-offs. So long as the system remains opt-in (whether centralized or decentralized), rather than the mandated approaches described below, it is likely to be ineffective. And even with a decentralized model, there are some privacy risks. The following lists four key flaws.

First, the system has to be widely utilized to be effective—something that is true for the government-run systems as well. In fact, one highly regarded study indicates that adoption by 56 percent of the population overall is needed for the apps to be effective.[31] Even in Iceland, which as of May 2020 had the highest per capita usage of an opt-in contact tracing in the world, usage rates then stood at about 38 percent.[32]

Second, as several scholars and technologists have noted, the kind of Bluetooth proximity tracing employed by the Google and Apple system is imprecise.[33] It can read signals through walls and sealed-off spaces, meaning it may not be able to distinguish between someone sitting across from another at a dinner table for 20 minutes and two people stuck adjacent to each other in a traffic jam, windows rolled up, for that same period of time. This translates into a risk of false positives. Conversely, it may fail to pick up a range of other potential transmissions, either because of insufficient app usage, or because of the failure to trigger warnings for contacts of very short duration that nonetheless lead to transmission of germs—meaning a risk of false negatives. So long as users recognize the gaps, this is not in and of itself a particular concern—after all, no contact tracing system is fool-proof. But if and when users presume that the technology is the magic solution, there is a possibility that people will operate based on a false sense of security and take more risky actions as a result.

Third, even if the system is designed with the best security protections available, no such system is invulnerable. It is at least possible that hackers could distort the system and send false alerts, creating alarm about new hot spots, potentially in strategically malicious ways, such as in the run-up to Election

30. Joint Statement from Scientists and Researchers on Contact Tracing, *supra* note 27.

31. ROBERT HINCH ET AL., EFFECTIVE CONFIGURATIONS OF A DIGITAL CONTACT TRACING APP: A REPORT TO NHSX 3 (2020), https://perma.cc/S9UD-SM53.

32. Bobbie Johnson, *Nearly 40% of Icelanders Are Using a COVID App—And It Hasn't Helped Much*, MIT TECH. REV. (May 11, 2020), https://perma.cc/S6K5-5X83.

33. *See, e.g.*, JAY STANLEY & JENNIFER STISA GRANICK, THE LIMITS OF LOCATION TRACKING IN AN EPIDEMIC 3-4 (2020), https://perma.cc/MV78-3VX5; Patrick Howell O'Neill, *Bluetooth Contact Tracing Needs Bigger, Better Data*, MIT TECH. REV. (Apr. 22, 2020), https://perma.cc/CSQ3-N5LP (noting that the accuracy of Bluetooth proximity data can be impacted by whether Bluetooth-enabled devices are oriented vertically or horizontally, the underlying operating systems, and the objects and surfaces in the surrounding environment); Ashkan Soltani et al., *Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis*, BROOKINGS INST. (Apr. 27, 2020), https://perma.cc/T9XV-3MU2 (cautioning that Bluetooth-based contact-tracing apps are susceptible to false positives of exposure in instances such as receiving a Bluetooth signal through a wall but where there was in fact low possibility of virus transmission); Catherine Stupp, *Coronavirus Tracking Apps Raise Questions About Bluetooth Security*, WALL ST. J. (Apr. 30, 2020), https://perma.cc/BKC3-KJHT (recalling that "[Bluetooth] wasn't designed to generate detailed, reliable data about proximity between devices," with one of the original Bluetooth engineers disclaiming that "[t]he accuracy is limited").

Day.[34] While Apple and Google assert that the continuously-on use of Bluetooth requires an opt-in to activate, the capacity is built into their operating systems, similarly creating at least the risk, even if small, of remote activation. The revelation that Google's phones require location services to be turned on in order for the Bluetooth system to work raises additional concerns. Even if the location data are not intentionally shared, they remain susceptible to unwanted and unplanned access.[35]

Finally, the systems only work well if they are part of a wider containment strategy, of which widespread and easily activated testing is the most important step. If those who receive an alert about a potential exposure cannot take steps to find out if they are themselves a disease vector, the system will likely have little effect.[36]

2. Quarantine Monitoring and Other Enforcement Mechanisms

A range of location tracking and other digital tools can support quarantine monitoring.[37] Poland, for example, launched "Home Quarantine" app, pursuant to which quarantined individuals are sent random requests to upload geo-located photos, thus proving they are in their home.[38] Hong Kong both tracked quarantined individuals' locations and required them to check in several times a day by means of an app.[39] At least one judge in the United States ordered the use of a GPS-located ankle bracelet on a man who failed to abide by a quarantine order in Kentucky.[40]

All such tools use surveillance as an enforcement mechanism. Some such uses are preventive, imposed on everyone subject to quarantines or other restrictions on their movements. Others, such as the ankle bracelet ordered in Kentucky, are reactive—a means of monitoring and enforcing in response to a demonstrated failure of compliance.

---

34. *See Hearing Statement*, *supra* note 13, at 4 (warning of various possible malicious uses, including a "foreign operative who wished to sow chaos, an unscrupulous political operative who wished to dampen political participation, or a desperate business owner who sought to shut down the competition . . . us[ing] self-reported instances of COVID-19 in an anonymous fashion to achieve their goals").

35. *See* Singer, *supra* note 29.

36. For a fuller discussion of these concerns, see Jennifer Daskal & Matt Perault, *The Apple-Google Contact Tracing System Won't Work. It Still Deserves Praise*, SLATE (May 22, 2020, 12:11 PM), https://perma.cc/M3V5-NJS5.

37. I use quarantine monitoring here to cover both preventive quarantine measures on those deemed at risk of becoming ill and isolation measures imposed on those who have been diagnosed as ill and thus contagious, although there are, of course, important differences between the two.

38. Isobel Asher Hamilton, *Poland Made an App that Forces Coronavirus Patients to Take Regular Selfies to Prove They're Indoors or Face a Police Visit*, BUS. INSIDER (May 23, 2020, 12:06 PM), https://perma.cc/L7G8-TLTD.

39. Mary Meisenzahl, *People Arriving in Hong Kong Must Wear Tracking Bracelets for 2 Weeks or Face Jail Time. Here's How They Work.*, BUS. INSIDER (May 4, 2020, 2:32 PM), https://perma.cc/5Z68-WP82.

40. Mallika Kallingal, *Ankle Monitors Ordered for Louisville, Kentucky Residents Exposed to COVID-19 Who Refuse to Stay Home*, CNN (Apr. 3, 2020 11:55 AM), https://perma.cc/BKE4-724M.

Digital tools also could be used to monitor and enforce compliance with social distancing and other analogous orders. Several states, for example, have issued orders limiting public gatherings to no more than specified numbers of people.[41] These, too, could be enforced via population-level analysis, individual tracking, or a combination of both.

3. Screenings

As workplaces, schools, and businesses reopen, there is an almost inevitable urge to screen and thereby sort the healthy from the sick. Possibilities include, among other things: remote digital temperature taking; digital system trackers, by which individuals self-report basic health information, something that some universities and others are demanding; and assignment of digital QR codes based on assessment of health risk. Other tools can be used for social distancing enforcement. One company, for example, has developed a wireless, wearable device that vibrates when another person, also wearing the device, gets too close.[42] Each of these is a new form of digital surveillance—in pursuit of public health goals.

II. WHETHER TO COMPEL?

In many parts of the world, health surveillance has been imposed top-down. Citizens in China, Israel, and South Korea, as just some examples of many, have been subjected to surveillance systems that tracked their movements and connections in an effort to minimize community spread.[43] And many have claimed better health outcomes as a result.[44]

In the United States, at least as of this writing, no federal or state entity has mandated broad-based location or proximity tracking for either contact tracing or

41. *See, e.g.*, Don Thompson, *California Governor: No Large Gatherings Due to Coronavirus*, U.S. NEWS (Mar. 12, 2020), https://perma.cc/YVD7-4GTM.

42. James Temple, *Prepare to Be Tracked and Tested as You Return to Work*, MIT TECH. REV. (May 22, 2020), https://perma.cc/9LU3-9KR3.

43. *See, e.g.*, Arjun Kharpal, *Use of Surveillance to Fight Coronavirus Raises Concerns about Government Power after Pandemic Ends*, CNBC (Mar. 16, 2020), https://perma.cc/HBM8-QNUT (describing pandemic-related surveillance regimes that have been adopted in various countries across the globe); Ruth Levush, *Israel Security Agency's Involvement in COVID-19 Tracing Scrutinized*, LIBR. OF CONG. (May 7, 2020), https://perma.cc/EH35-XD6C.

44. *See, e.g.*, Aaron Holmes, *South Korea Is Relying on Technology to Contain COVID-19, Including Measures That Would Break Privacy Laws in the US—and So Far, It's Working*, BUS. INSIDER (May 2, 2020, 12:30 PM), https://perma.cc/3SPL-BKDY (suggesting that digital contact tracing and digitally-enforced quarantine requirements helped keep caseloads low in South Korea); HINCH ET AL., *supra* note 31, at 17-20 (emphasizing the potentially substantial impact of digital contact tracing in halting the spread of the disease, made more effective the higher the uptake). Surveillance, however, cannot be looked at in isolation. There is a critical interplay between surveillance and other means of disease control, including widespread and available testing, something the United States lacks. *See, e.g.*, Isobel Asher Hamilton, *Iceland Had the Most-Downloaded Contact-Tracing App for Its Population Size. Authorities There Say It Hasn't Made Much Difference.*, BUS. INSIDER (May 12, 2020, 10:40 AM), https://perma.cc/TE7D-J3EF (discussing how Iceland halted the spread via a combination of aggressive contact tracing, much of which is done by humans, and widespread testing).

preemptive quarantine enforcement purposes.[45] Nonetheless, mandatory health screenings are almost certain to follow, at least as a condition for engaging in certain sought-after activities. (Already it is something that many employers are requiring.[46]) And universally mandated contact tracing and quarantine enforcement are all tools that may be contemplated in the future—either in connection with COVID-19 or as a means of control in the wake of a future pandemic. The following considers whether, and in what circumstances, the kinds of collection discussed in Part I could be mandated. The following sections focus first on the law and then on the policy. Of course, in reality, the two are intertwined.

A. The Legal Issues

This section focuses primarily on the Fourth Amendment as the key constitutional provision that regulates government data collection.[47] It briefly addresses both due process and First Amendment considerations, albeit in a cursory way. This section also notes both the Electronic Communications Privacy Act[48] and Telecommunications Act,[49] as they both address whether and in what circumstances covered tech and telecommunications providers may share relevant data, even in the absence of a direct government mandate.

1. The Fourth Amendment—A Limited Constraint

The Fourth Amendment protects against unreasonable searches and seizures by government officials—generally requiring a warrant as a pre-condition for searching and seizing. But not always. It does not prohibit the voluntary sharing of data with the government, and it does not generally govern private actors (such as tech companies or private employers), although in some cases private actors can be treated as state actors and thus bound by the Fourth Amendment.[50] It does, however, control government actors, raising the question of what kinds of surveillance schemes are and are not constitutionally permitted for purposes of health surveillance. The quick answer: A whole lot, but not everything. The greater the privacy protections, the more careful the program design, the greater tailoring of

45. The CDC has been given large dollars for "health surveillance." Adam Klein & Edward Felten, *The 9/11 Playbook for Protecting Privacy*, POLITICO (Apr. 4, 2020, 11:11 AM), https://perma.cc/C6M5-PFKF. These dollars, however, appear to be used to support traditional health surveillance—meaning collection of information about disease incidents and syndromic surveillance, referring to the tracking of symptoms as opposed to confirmed cases—rather than to track movements or contacts of individuals.

46. Phil Galewitz, *Some Employers May Require Employees Get Tested for COVID-19 Before Coming Back to Work*, TIME (May 7, 2020, 1:18 PM), https://perma.cc/2CGC-NQHB (discussing employers' plans to require employees to fill out questionnaires about their health and travel history, have their temperature taken, and submit to diagnostic tests for the virus).

47. U.S. CONST. amend. IV.

48. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

49. 47 U.S.C. §222 (2018).

50. For a discussion of this issue, see, *e.g.*, Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID-19*, 7 J. L. & BIOSCIENCES 1, 8-9 (2020).

program to need, the more likely any new surveillance system will be deemed constitutional.

The Fourth Amendment analysis starts with the core question: Was there a "search"? The Fourth Amendment definition of search is a term of art. There needs to be either a trespass into a constitutionally protected space, such as the home, or a violation of what is known as a "reasonable expectation of privacy," which is in and of itself a socially constructed and shifting concept.[51] For years, the government advocated a sweeping conception of what is known as the third-party doctrine—basically arguing that individuals lose a reasonable expectation of privacy in all information that has been shared with others—including location data in the hands of tech companies that use such data to do things like transmit goods or services to their users. In the 2018 case of *Carpenter v. United States*, however, the Supreme Court placed key limits on that doctrine, ruling that individuals maintain a reasonable expectation of privacy, and thus that the Fourth Amendment applies to, a week's worth or more of their cell-site location data in the hands of third party cell phone providers.[52]

Given *Carpenter*, the mandated collection of a week or more of location history—the kind needed for contact tracing or quarantine monitoring—triggers application of the Fourth Amendment.[53] And while the *Carpenter* Court emphasized that it was focused on the particular facts before the Court, the reasoning applies equally to the kind of proximity data obtained via Bluetooth tracking as well.[54] Like the location data at issue in *Carpenter*, Bluetooth-enabled tracing creates a "detailed, encyclopedic, and effortlessly compiled" mapping of

51. *See* United States v. Jones, 565 U.S. 400, 409 (2012) (making clear that the "trespass" test is alive and well); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (establishing the "reasonable expectation of privacy"); Alan Z. Rozenshtein, *Disease Surveillance and the Fourth Amendment*, LAWFARE (Apr. 7, 2020, 1:54 PM), https://perma.cc/6V3C-S3HK (providing a great explanation of how the Fourth Amendment applies to health surveillance). For critiques of the reasonable expectation of privacy test, *see* Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting) ("[W]e still don't even know what [*Katz*'s] 'reasonable expectation of privacy' test is. Is it supposed to pose an empirical question . . . or a normative one . . . ? Either way brings problems."); *Jones*, 565 U.S. at 427 (Alito, J., concurring) (critiquing the *Katz* test for "rest[ing] on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations"); Erik Luna, *The* Katz *Jury*, 41 U.C. DAVIS L. REV. 839, 846 (2008) (scrutinizing the Court's post-*Katz* decisions as "outcome-based jurisprudence" that use "haphazard" and inconsistent analyses).

52. *Carpenter*, 138 S. Ct. at 2217 n.3.

53. *See, e.g.*, Grady v. North Carolina, 575 U.S. 306, 310 (2015) (use of a GPS-enabled ankle bracelet constitutes a search); Demo v. Kirksey, No. 8:8-cv-00716-PX, 2018 WL 5994995, at *3, *5-6 (D. Md. Nov. 15, 2018) (relying on *Carpenter* to find a reasonable expectation of privacy against six months of constant GPS surveillance); Pennsylvania v. Pacheco, No. 151 EDA 2018, 2020 WL 400243, at *9 (Pa. Super. Ct. Jan. 24, 2020) (recognizing a reasonable expectation of privacy in real-time cell-site location data, finding "no meaningful distinction between the privacy issues related to historical and real-time CSLI"); *see also* Motion to Suppress Evidence Obtained from a "Geofence" General Warrant, United States v. Chatrie, No. 3:19-cr-00130-MHL, 2019 WL 7660969 (E.D. Va. filed Oct. 29, 2019) (asserting a reasonable expectation of privacy in Google Location History data—location data derived from a collection of cell site data, GPS signals, and proxy to Wi-Fi networks and Bluetooth devices—acquired by means of a geofence warrant).

54. *Carpenter*, 138 S. Ct. at 2220 (describing its opinion as a "narrow one").

associations over time, generating access to "retrospective" and "otherwise unknowable information"—thereby bringing it within the Fourth Amendment's ambit.[55]

Carpenter involved the targeted collection of a particular individual's location history. Whether or not—and in what circumstances—the rule applies to mandated collection of aggregate-level, anonymized data is unsettled. The analysis turns to a significant extent, on the risk that the anonymized data could be de-anonymized or combined with other data sets to reveal personal and "otherwise unknowable" information about individuals, thereby triggering the same concerns at issue in *Carpenter*, even if initially shared in a way meant to protect individuals' privacy.[56]

A range of other screening programs directly mandated and implemented by government actors also appear to fall within the Fourth Amendment's mandate, although the specifics matter. While the Supreme Court has not yet ruled on the issue, it seems likely (and also the right outcome) that remote temperature taking and other non-consensual health screenings would be deemed a Fourth Amendment search—something that impinges on private personal information and thus a "reasonable expectation of privacy."[57] The Court has, after all, concluded that a heat detector used to remotely detect the temperature inside of a home was a search; it seems that the use of a remote thermometer to detect body temperature would be deemed a search of a person.[58] In other cases, it has

55. *Id*. at 2216, 2218; *see also* Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT 27, 43-45, 48 (Paper No. 18-29, forthcoming) (interpreting Carpenter to extend Fourth Amendment protections to transactional records revealing how an online messaging service was used and the IP addresses of websites visited); Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1164 (2018) (viewing *Carpenter* as affirming that the government conducts a search when it "uses technologies or investigative techniques that facilitate a broad, continuous, and indiscriminate collection of personal data that intrudes upon reasonable expectations of quantitative privacy"); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 359 (2019) (positing that the reasoning Carpenter applies could readily apply to "databases of web browsing habits stored by internet service providers," telephone and banking records, automated license plate readers, data collected by home-IoT devices, and troves of information entrusted to cloud providers); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 YALE L.J. F. 943 (2019); Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209 (2019) (asserting that *Carpenter* supports a distinct expectation of privacy based on the granularity of sought-after data that, in turn, supports an reasonable expectation of privacy in online browsing history).

56. *Enlisting Big Data in the Fight Against Coronavirus: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 116th Cong. 11 (2020) (written answers of Leigh Freund, CEO, Network Advertising Initiative) ("In an era of big data, super computers and highly sophisticated hackers, even using sophisticated anonymization techniques cannot completely prevent the possibility of anonymized data being associated with an individual."); Ira S. Rubinstein & Woodrow Hartzog, *Anonymization & Risk*, 91 WASH. L. REV. 703, 711-13 (2016) (highlighting shortfalls in anonymization techniques and how auxiliary information can be used to re-identify large data sets).

57. *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring).

58. Kyllo v. United States, 533 U.S. 27, 40 (2001) (use of a heat detector monitor, albeit heat emanating from the home rather than a person, constituted a search). That case, however, turned in part on the fact the technology was in "general public use." *Id*. at 34. To the extent certain types of screening, like remote thermometers, become widely available, some might argue that there is no longer a Fourth

concluded that things like compelled uses of breathalyzers to detect blood alcohol content are searches, albeit concluding that in a range of cases their warrantless use is permitted.[59]

Of course, the fact that something is a search does not mean that it is prohibited. It means that it needs to be "reasonable." Of particular relevance here is what is known as the "special needs" doctrine, to which I now turn.

2. Special Needs Searches

In a variety of different cases, the Supreme Court has upheld suspicion-less searches—such as highway checkpoints to identify drunk drivers—on the ground that they satisfy a "special need" different from traditional law enforcement.[60] Key factors: whether or not the government has identified a legitimate health or safety need; whether the program is tailored to the stated special need; and the degree of intrusion into privacy and other civil liberties. The final two factors are balanced against the stated state interest.[61]

While some have suggested that the doctrine allows the Court to uphold what they like and strike down what they don't like—mostly upholding whatever the government wants—that is too cynical a read of the Court.[62] While it is true that the Court has allowed broad-based programmatic surveillance in response to claimed "special needs," what is permitted does have limits, even if few. Of note, the Court has rejected application of the special needs doctrine to programs and policies that give government officials too much discretion to arbitrarily search; have a "primary" law enforcement purpose; or are too "entangle[d]" with law enforcement, as evidenced by law enforcement involvement in program design.[63] The Court's case law has set out a relatively clear road map as to how to design a "special needs" surveillance program that survives Fourth Amendment scrutiny. Step one: Identify a health or safety need separate and apart from law enforcement. Step two: Design a program tailored to that need. Step three: Limit intrusions into privacy and civil liberties, including, among other things, by avoiding arbitrariness in application.

Protection against disease spread in the face of a pandemic clearly fits the requirement of step one. This leads to steps two and three: First, is the program appropriately tailored to need? And second, how great is the intrusion into liberty

---

Amendment search. That, however, would, in my view, be an error, given—among other things—the fact that such screenings would in effect be a search of the body that reveals personal health information.

59. Birchfield v. North Dakota, 136 S. Ct. 2160 (2016).

60. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 449-50 (1990).

61. *Id.* at 455; *see also* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 297-98 (2016) (alleging that this balancing is "illusory" where "the overarching goal of a search scheme" is weighed "against a single individual's privacy interest").

62. *See, e.g.*, Christopher Slobogin, *Government Dragnets*, 73 L. & CONTEMP. PROBS. 107, 119 (2010); *see also* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 262-70, 277 (2011) (detailing the government's increased use of dragnet searches).

63. Ferguson v. City of Charleston, 532 U.S. 67, 82-84 (2001); City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000); Delaware v. Prouse, 440 U.S. 648, 663 (1979).

and privacy? The greater the intrusion, the less likely it will satisfy constitutional muster.

a. The Tailoring Question

The tailoring question requires careful consideration of the specifics, including the technology being used. Comprehensive surveillance schemes, of the type employed in South Korea (and of course China) provide the most accurate data, but with significant cost to privacy and other civil liberties. Other forms of collection will not be as precise. Contact tracing via cell-site location data, as was done in Israel, for example, is not likely to be particularly effective—yielding more precise locatoin information for those in places with closely spaced cell towers than in locations where such towers are spread far apart, and not particularly precise in either event.[64] GPS tracing is more precise, but raises greater privacy and other civil liberties concerns, thereby triggering potential worries about the degree of intrusion.[65] And while Bluetooth proximity tracking alleviates some of the privacy concerns related to GPS and other location data, it too can yield a high number of false positives if, for example, there is no mechanism to distinguish proximity of two individuals sitting across from each other over dinner and two people equally close together in a traffic jam or on opposite sides of a wall in a small apartment building.

Assessment of tailoring also requires an analysis of how such a program fits into a broader containment strategy. For quarantine monitoring, this is relatively straightforward. The surveillance serves a straightforward purpose—to track movements and thereby support enforcement of whatever quarantine rules are in place. In order to satisfy the tailoring requirement, such tracking should, if adopted, only be permitted for the period of the quarantine. And data should be destroyed when the quarantine period is over.

Contact tracing is more complicated. It is one thing to develop a strategy for notifying individuals that they have been in the vicinity of others who are sick. But to what aim? What are those deemed to have been in contact with sick individuals supposed to do? Get tested? If so, are there sufficient tests available and accessible—and at what cost? Are they free or subsidized for those who cannot

64. Reply to Brief in Opposition at 7, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (acknowledging that the precision of cell site data is impacted by the varying sizes of cell site sectors); STANLEY & GRANICK, *supra* note 33, at 3.

65. *See Jones*, 565 U.S.at 415-16 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)) (noting that GPS surveillance generates "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and that the government can store and mine such record years after its collection); Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 355 (2014) (breaking down how GPS technology enables the government to conduct mass surveillance that was previously impossible); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 458-59 (2007) (illustrating how GPS surveillance's sense augmentation, comprehensiveness, and pervasiveness enables the government to compile "a comprehensive digest of [one's] friends, associates, preferences, and desires").

afford them? Is there a self-quarantine requirement, while individuals await test results, or just in general because there are no available tests? For how long?

The higher the rate of false positives, the greater the number of individuals who are subject to the testing or quarantine requirement who are not actually sick, and the less tailored the scheme to the need.

b. The Degree of Intrusion

The possibility of mandatory testing and mandatory quarantines leads directly to the next inquiry—the degree of intrusion. Even mandatory testing can be a significant intrusion on liberty, particularly if individuals get frequent positive contact alerts, thus requiring those pinged to stop whatever they are doing, go to a testing center, and wait for the results. Quarantines impose a significant and dramatic deprivation of liberty—a far cry from the very brief traffic stop at issue in the seminal special needs case of *Michigan Department of State Police v. Sitz*.[66] The degree of intrusion also varies based on the technology used and core questions as to how collected data are handled. Critical to any such program are key questions of who can access collected data and for what reasons, how securely it is stored, and how long it is retained—all issues that matter greatly to an assessment of the degree of intrusion.[67] Any such program should, as a result, include the following: strict limitations on who can access the data and for what reasons; oversight and transparency to protect against error and abuse; strong security measures to protect against unauthorized access; and retention limits, so that data are not retained for longer than needed for the stated purpose—meaning approximately 14 days for both contact tracing purposes and quarantine monitoring.[68] As

66. *Sitz*, 496 U.S. at 448 ("The average delay for each vehicle was approximately 25 seconds."); *cf.* Jacobson v. Massachusetts, 197 U.S. 11, 28 (1905) (upholding mandatory smallpox vaccination program, but also emphasizing that public health mandates that intrude on liberty interests can only be justified if deemed "necessary," do not extend "beyond what [is] reasonably required for the safety of the public," and are not exercised in "an arbitrary, unreasonable manner"). *See also* Jew Ho v. Williamson, 103 F. 10, 26 (C.C.N.D. Cal. 1900) (striking down quarantine as overbroad and discriminatory, and as a result "unreasonable, unjust, and oppressive").

67. *See, e.g.*, David Kaye, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. on Disease Pandemics and the Freedom of Opinion and Expression, to Human Rights Council, U.N. Doc. A/HRC/44/49 at ¶¶54-57 (Apr. 23, 2020), https://perma.cc/R6F3-VVJV (noting that proper resolution to these issues, among others, requires ensuring that health surveillance complies with international human rights law); EUR. DATA PROT. BD., GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK 7-9 (2020), https://perma.cc/SW5B-YZ5A (discussing extensively data privacy and security considerations pertaining to contact tracing apps and highlighting that "the health crisis should not be used as an opportunity to establish disproportionate data retention mandates"); STANLEY & GRANICK, *supra* note 33, at 2 (identifying five variables influencing the effectiveness of using cell phone location data to combat coronavirus spread); Andrew Crocker et al., *The Challenge of Proximity Apps for COVID-19 Contact Tracing*, ELECTRONIC FRONTIER FOUND. (Apr. 10, 2020), https://perma.cc/ZAF4-FU5Q (listing consent, data minimization, information security, transparency, bias, and expiration as necessary safeguards for contact tracing proximity apps).

68. Ideally, for policy reasons laid out below, the data would be used exclusively for public health purposes, although cases like Sitz make clear that this may not be constitutionally required, so long as the initial information gathering was done for non-law enforcement reasons.

is perhaps evident, decentralized storage systems, of the kind envisioned by the Apple-Google system, raise fewer concerns than systems that result in new databases of personal data. Decentralized systems may, however, be less effective in that they do not share with health officials potentially critical information.

This assessment of intrusion also needs to grapple with at three additional considerations: i) the fact that any quarantine monitoring or contract tracing system will almost inevitably involve monitoring of activities in the home—a locus that has been given special protection in Fourth Amendment jurisprudence;[69] ii) requirements that individuals take affirmative steps to assist with the surveillance, in ways that trigger due process considerations; and iii) related but independent First Amendment considerations associated with mapping of association.[70]

As to the first, the potential intrusion into the home, the Supreme Court has upheld "special needs" searches into individuals' homes in prior cases.[71] Such cases have turned, in significant part, on the target's diminished expectation of privacy, given, for example, the target's status as a probationer or parolee.[72] Preemptive quarantine monitoring and contact tracing, by contrast, involve surveillance in the home in a broad-based way—not just for arrestees or others deemed (whether rightly or wrongly) to have diminished privacy rights. In the separate, but related category of administrative searches for purposes of monitoring compliance with health and safety codes, the Court has allowed a relaxation of the "probable cause" requirement, instead allowing searches to proceed based on a

69. *See, e.g.*, Florida v. Jardines, 569 U.S. 1, 6 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals."); *id.* at 13 (Kagan, J., concurring) (noting the ways in which "property concepts and privacy concepts . . . align" in cases involving searches of homes); *Kyllo*, 533 U.S. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."); Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (upholding aerial surveillance of commercial property, yet noting that "[i]t may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant"); Donovan v. Dewey, 452 U.S. 594, 598 (1981) (contrasting a permissible administrative search of commercial premises with that of private homes, and emphasizing that the latter "generally must be conducted pursuant to a warrant in order to be reasonable under the Fourth Amendment").

70. In this I consider both the due process and First Amendment considerations in connection with the special needs balancing test, and, in particular, assessment of intrusion. It is important to emphasize that each also serves as a stand-alone limitation on mandatory contact tracing—and each thus deserves much greater treatment than I give it here. The First Amendment considerations are particularly potent and potentially heighten the degree of scrutiny applied.

71. Griffin v. Wisconsin, 483 U.S. 868, 873-74, 880 (1987) (noting that "special needs" beyond normal law enforcement may justify departures from the usual warrant and probable cause requirements, and holding that Wisconsin's statutory scheme—pursuant to which probation officers could engage in a warrantless search of a probationer's home based on "reasonable grounds" that there was contraband present—satisfied the Fourth Amendment).

72. *Id.* at 875-76; *see also* City of Los Angeles v. Patel, 576 U.S. 409, 424-26 (2015) (rejecting a far-reaching application of the related administrative search outside of a small subset of "closely regulated" industries—namely liquor stores, firearm dealers, mining companies, and automobile junkyards—highlighting the Court's aversion to expansive applications of the special needs doctrine and its cousins to justify warrantless intrusions into constitutionally protected spaces).

"reasonable" standard. But the Court has also made clear that the warrant requirement continues to apply, albeit pursuant to a lessened standard.[73]

It is certainly possible that protecting the population in the midst of a pandemic may be deemed a sufficiently weighty need to justify a warrantless intrusion into the home. Nonetheless, home monitoring will almost certainly be understood as a greater intrusion than monitoring outside the home, and thus require a greater tailoring of program to need than might otherwise apply.

Moreover, in at least some cases, such surveillance schemes will operate via an affirmative demand to either download and activate an app or wear some sort of surveillance device. In such cases, individuals are not just being passively surveilled, but are required to take affirmative steps, on an ongoing basis, to help support and enable such surveillance. To be sure, courts have routinely ordered and permitted things like ankle bracelet monitoring and drug testing, but the scope and application have been limited. Ankle bracelets are generally ordered in response to an individualized assessment of things like flight risk pending trial or an assessment of danger—considerations that courts have routinely held justified greater intrusions on liberty than would otherwise be permitted.[74] Drug testing programs also have been permitted as a condition of participation in a voluntarily-chosen activity, like an extracurricular sport, or as a means of ensuring compliance with particular employment requirements.[75] Broad-based, across the board requirements that individuals *do* something—*e.g.*, download and activate an app, wear or constantly carry some sort of monitoring device information—raise potential due process concerns.[76] Moreover, a requirement that individuals download and activate an app onto their phones potentially operates as a "seizure" of a person's effects.[77]

Any such program that requires self-reporting, a form of compelled speech, also potentially triggers the First Amendment. The mapping of movements and associations also raises significant First Amendment considerations.[78] Unlike

---

73. *See, e.g.*, Camara v. Municipal Court, 387 U.S. 523 (1967).

74. Ava Kofman, *Digital Jail: How Electronic Monitoring Drives Defendants Into Debt*, PROPUBLICA (July 3, 2019, 5:00 AM), https://perma.cc/L4WD-5S7Y.

75. *See, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 825-26, 838 (2002) (upholding a school board drug testing policy requiring high school and middle school students to take a drug test before participating in an extracurricular activity, submit to random drug testing while participating in such activity, and agree to be tested at any time upon reasonable suspicion); Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 679 (1989) (upholding as reasonable the "suspicionless testing of [U.S. Customs Service] employees who apply for promotion to positions directly involving the interdiction of illegal drugs, or to positions that require the incumbent to carry a firearm").

76. *See also* Alan Rozenshtein, *Digital Disease Surveillance* (manuscript at 11) (forthcoming) (suggesting that requiring someone to download an app might separately trigger the Fourth Amendment under the *Jones* trespass test).

77. *See* Ram & Gray, *supra* note 50, at 10-11.

78. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (warning that the "[a]wareness that the Government may be watching chills associational and expressive freedoms," and noting the interactions between Fourth and First Amendment considerations in any tracking program); *see also* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE

surveillance schemes adopted to track terrorist suspects, such surveillance will presumably be transparent. This means two things: first, the standing issues which bedeviled so many legal challenges associated with terrorism surveillance schemes are largely eliminated; the surveillance is not speculative—it is overt.[79] Second, the chilling effect is likely even greater; individuals will not just think they might be watched, they will *know* they are being watched. These considerations are important both for any separate and independent First Amendment claims and for assessing the degree of intrusion imposed.

Finally, it is worth noting that while this discussion has largely focused on quarantines and contract tracing, the same analysis applies to screening programs as well. Such screening programs are evaluated on similar terms as other health surveillance schemes—balancing the government interest, tailoring of the program, and degree of intrusion. Drunk driving roadblocks, metal detectors as a condition of entry into a range of governmental buildings, and airport security measures are all examples of screening mechanisms employed and upheld as constitutional—albeit in some cases labeled as "administrative" as opposed to "special needs" searches.[80] A range of health monitoring, such as remote temperature taking, could be implemented for similar health and safety reasons. As with other surveillance programs, the details matter, including an assessment and balancing of need, tailoring, and intrusiveness. Does heightened temperature taking actually provide useful data? What about the false positives—people who have a heightened fever but not a communicable disease? And false negatives—the many asymptomatic people that such screening misses?

To be clear, the Supreme Court has never required a perfect correlation of data to relevant fact, but a sufficiently high degree of false positives and false negatives raises undoubted questions about tailoring to need. And once again, there are core questions as to what comes next. Are those with fevers prohibited from public transport or entry into government buildings? As the rates of false positives increase, this would be a burden on liberty that could be fatally overinclusive. Other features of program design, including the question of who has access to the data, how long is it retained, how securely is it held, and how is it disseminated, all come into play. Such data, if tied to facial recognition technology or

---

SURVEILLANCE COURT 132-36 (2014), https://perma.cc/H6KQ-65JR (discussing First Amendment implications of telephony metadata program, which, akin to contract tracing efforts, tracked associations over time); Jonathan W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 124-25, 140, 152 (2016) (analyzing the sudden drop in views and viewing trends of "privacy-sensitive" Wikipedia articles—those "correspond[ing] with DHS keywords listed as relating to 'terrorism'"—concluding that such viewership changes are "consistent with a significant and long-term chilling effect").

79. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 418 (2013) (concluding that "fear of surveillance" again was not sufficient to create standing); Laird v. Tatum, 408 U.S. 1 (1972); Montgomery v. Comey, 752 F. App'x 3, 4 (D.C. Cir. 2019) ("A subjective fear of surveillance, without more, is insufficient to confer standing to bring a First Amendment challenge to a surveillance program."); United States v. Moalin, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013).

80. Primus, *supra* note 62, at 255-56, 259-60 (arguing that "administrative searches" emerged from the conflation of "dragnet intrusions" and "special subpopulation searches").

other individually identifying data, could, if retained, operate as a new form of location mapping. Once the key decision is made—e.g., to allow or deny entry into a government building—any such data should be destroyed.

3. Targeted Surveillance

Thus far, our discussion has focused on suspicionless searches. But some such surveillance may in fact be based on individualized suspicion. At least one court (in Kentucky) has ordered electronic monitoring in response to a demonstrated failure to comply with a quarantine order, for example. This is a significant restriction on liberty.[81] But, as with civil commitment orders, it would seem to fall squarely within the state's protective powers, so long as it is imposed based on a neutral and fair-minded presentation of facts, employed in an impartial and non-discriminatory or arbitrary way, and time-limited to the 14-day quarantine period for which the monitoring is needed for quarantining purposes. Other steps to minimize the effect on other core rights and liberties—including deletion of the relevant data after a quarantine is lifted, the adoption of strong data security protocols, and effective oversight and transparency—are both good policy and also help support the program's legality.

4. Voluntary Data Disclosure Regimes

The Fourth Amendment regulates governmental searches of data. It does not bind or otherwise limit private collection of data. Nor does it prohibit the voluntary sharing of data that could not, pursuant the Fourth Amendment, be directly man-dated. The Electronic Communications Privacy Act (ECPA)—covering the disclosure of certain stored data—and the Telecommunications Act—covering data collected by telecommunication and broadband providers—fill this gap, regulating the private actors that hold the data and setting strict limits on disclosure of that data. Still, these statutes are subject to numerous gaps and exceptions. As statutes, they could be amended so long as the amendments satisfy the Fourth Amendment and other constitutional rules.

ECPA prohibits voluntary disclosures of stored data, absent a specified statutory exception. For non-content data (including location and proximity data) there are six such exceptions to the prohibition on voluntary disclosure. Two are relevant here: disclosure with user consent, and in specified emergencies.[82] User consent will be applicable in only a small number of cases. The emergency disclosure provision requires a finding that there is a danger of death or serious

81. *See* Raphael Satter, *To Keep COVID-19 Patients Home, Some U.S. States Weigh House Arrest Tech*, REUTERS (May 7, 2020, 8:08 AM), https://perma.cc/6RX4-7WHJ ("We don't want to take away people's freedoms but at the same time we have a pandemic," quoting Amy Hess, Chief of Public Services, Louisville, Ky.).

82. *See* 18 U.S.C. §2702(c)(2), (4) (2018). Other exemptions include disclosure to providers as may be necessary to render service or protect its rights or property, to the National Center for Missing and Exploited Children, to any person other than a governmental entity, to a foreign government subject to a congressionally certified executive agreement, or as authorized in §2703. *Id.* §2702(c)(3), (5), (7).

physical injury that "requires disclosure without delay."[83] While the emergency exception could be relied on in narrow, specific cases—if, for example, health authorities were seeking to track down a person who tested positive and was defying a quarantine order in ways that authorities feared put community members at risk—it would be a stretch to claim that this exception permits wide-spread sharing of data for preventive health purposes.

Notably, ECPA only applies to specified covered service providers—namely "electronic communication service" (ECS) and "remote communication service" (RCS) providers.[84] These definitions cover email service providers, social media companies, text messaging services, and a range of different tech companies that provide data communication and storage tools directly to the public.[85] They exclude, however, researchers, analysts, and data brokers, among many others that fail to meet the definitions of covered providers—even if they have bought or otherwise been provided data by ECPA-covered providers. These non-ECPA-covered providers are not bound by ECPA-imposed limitations on the sale, transfer, or disclosure of non-content data to third-parties, although they may be subject to separate state or sectoral privacy laws that limit disclosure.[86]

The Telecommunications Act similarly sets limits on the voluntary disclosure of personal data, including location data.[87] In a never-concluded FCC proceeding, a group of privacy advocates charged AT&T with violating the non-disclosure

83. 18 U.S.C. §2702(c)(4) (providing an exception to the disclosure prohibition "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency"). While COVID-19, as well as future pandemics, involve the "danger of death," this provision does not and has not been previously understood to justify the wide-spread sharing of data for preventive purposes.

84. 18 U.S.C. §2510(15) ("'[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications."); 18 U.S.C. §2711(2) ("'[R]emote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.")

85. *See, e.g.*, Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (concluding that the statutory definition of an ECS includes basis e-mail services); Quon v. Arch Wireless, 529 F.3d 892, 901 (9th Cir. 2008) (holding that a provider of text-messaging pager services is an electronic communications service provider), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 560 U.S. 746 (2010); *In re* United States for an Order Pursuant to 18 U.S.C. 2705(B), 289 F. Supp. 3d 201, 203 (D.D.C. 2018) (concluding that Airbnb is an "ECS provider under the SCA by virtue of the electronic messaging system it provides to users of its service"); Ehling v. Monmouth-Ocean Hosp. Serv., 961 F. Supp. 2d 659, 667 (D.N.J. 2013) (holding that Facebook, a social media network, is an electronic service provider); *In re* Search Warrant for [Redacted].com, 248 F. Supp. 3d 970, 974 (C.D. Cal. 2017) (concluding that a "cloud computing service such as Adobe" is an RCS); Viacom Int'l, Inc. v. YouTube, Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (establishing that YouTube is an RCS).

86. Meanwhile, even ECPA-covered providers can share the kind of aggregated, population-level analysis of the kind being compiled by Facebook, Google, and Apple without running afoul of ECPA. When aggregated in sufficiently large data sets, it is not data that would "pertain" to a customer or subscriber—and thus is not subject to the limitations on disclosure. If, however, the entities were to share underlying data, that would run afoul of the disclosure limits. There is an open question as to whether and to what extent de-identification tools could sufficiently limit that risk to avoid ECPA limits on disclosure.

87. 47 U.S.C. §222 (2018).

provision when it sent anonymized user data to the CIA.[88] Petitioners warned that anonymized data could be de-anonymized, and asserted that the data could only be shared if aggregated in ways that fully removed individual identifies and characteristics.[89] AT&T countered that it was employing best practices designed to protect the identity of their users, and could share the de-anonymized and de-identified data consistent with the Act.[90] The dispute was never resolved, but nonetheless made clear that even the sharing of carefully scrubbed de-identified data sets carries risks.[91]

III. THE POLICY CONSIDERATIONS

Tracking, tracing, and screening, albeit primarily of the human-to-human form, has long played a critical role in preventing and minimizing disease spread. It is both natural and inevitable—and in many cases beneficial—that technology be used to augment these long-standing means of containment and control. Nevertheless, it also is dangerous to assume that technology will be the "knight in shining armor."[92] It should be employed in ways that promote good health, but it should—particularly give the risk that technologies adopted and data collected for one purpose get co-opted and employed for others—be done with care. The relevant players should, among other things, employ the best principles of privacy by design. The technology should employ best practices with respect to data security and data minimization. And policy makers should insist on effective transparency, accountability, and oversight mechanisms. Even then, some uses of the technology will still not make good sense.

These principles are not only good for privacy, they are also good for health. People will not employ technologies if they do not trust them. That requires, among other things, trust in how personal data are handled and protected. People also will not seek out the public health assistance they need if they fear the

88. Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers without Customers' Consent Violates Section 222 of the Communications Act (filed Dec. 11, 2013) (FCC Dkt. No. 13-306), https://perma.cc/QL4T-LKTK [hereinafter Petition of Public Knowledge et al. for Declaratory Ruling].

89. *Id*. at 5 (citing 47 U.S.C. §222(h)(2) and contrasting the definitions of "aggregate customer information" and "individually identifiable customer proprietary network information" in the statute).

90. Comments of AT&T, Petition of Public Knowledge et al. for Declaratory Ruling (filed Dec. 11, 2013) (FCC Dkt. No. 13-306), https://perma.cc/F8C2-D9XH.

91. Finally, it is impossible to discuss health surveillance without at least mentioning the Health Insurance Portability and Accountability Act (HIPAA), which protects the privacy of medical records and thus has relevance for assessing when and in what situations the health status of particular individuals may be disclosed (and then tracked) by covered entities. But it includes a vast carve-out—enabling disclosure of health information to public health authorities for, among other things, health surveillance purposes. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C. and 42 U.S.C.); *see also* 45 C.F.R. §164.512 (b), (f), (j) (2020) (covering uses and disclosures for public health activities, law enforcement purposes, and to avert a serious threat to health or safety, respectively); OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., DISCLOSURES FOR PUBLIC HEALTH ACTIVITIES [45 CFR 164.512 (b)] (2002), https://perma.cc/8GVL-3PZR.

92. Daskal & Perault, *supra* note 36.

tracking and monitoring that comes with it. Once one moves to mandatory, as opposed to voluntary, uses of technology, the use of effective privacy protections, coupled with a close tailoring of program to need, may also be the key to its legal viability as well as good policy.

With these principles in mind, I suggest a few core considerations.[93] First, a narrow tailoring of scheme to purpose. This requires assessment of the ways in which the technology does (or does not) serve the public health goals—what is often called the "proportionality" analysis, but which requires a deep dive into the full array of key considerations and applications.

Second, a resistance to the creation of new databases, whether private or governmentally-held. As the Apple and Google system, as well as those of other app developers, has demonstrated, key data can, depending on the program and purpose, be held in a decentralized way without the generation of new databases. This should be employed wherever possible. Of course, decentralized systems will not serve many screening or quarantine enforcement efforts' goals, in which case systems, if they are employed, will need to be centralized. That triggers the need for carefully crafted protections with respect to access, use, and retention, as the next set of recommendations discusses.

Third, clear limits on data retention, so that acquired data are not kept longer than needed. This is important no matter what, but particularly important as new data sets are being quickly created and generated in response to a perceived emergency need.

Fourth, clear limits on how collected data are used and with whom they are shared, along with penalties for disclosures that fail to meet these requirements. Already, reports indicate that a contract tracing app implemented by North and South Dakota shared private information with an outside company, in violation of its own privacy policies.[94] This unauthorized sharing of information should be sanctioned as a violation of both privacy and good public health; people will be less willing to trust systems that fail to abide by their promises. And while this discussion is focused on data collected for public health reasons, there will be an almost inevitable interest in these data by others, including law enforcement and possibly intelligence officials. This should be resisted, if for no other reason, because it will make the populace more distrustful of public health programs.

Fifth, strong security protocols to protect the integrity of the data, regardless of how they are maintained. This is necessary to protect against malicious hacks into and uses of the data; it is also critical to prevent against malicious actors using the systems to disseminate faulty information in ways designed to sow general chaos or serve other economic or geopolitical goals.

Sixth, a strong and healthy wariness of government-mandated contract tracing and preemptive quarantine. Even if designed with care, the risks of mission creep

93. STANLEY & GRANICK, *supra* note 33, at 2.

94. *See* Geoffrey Fowler, *One of the First Contact-Tracing Apps Violates Its Own Privacy Policy*, WASH. POST (May 21, 2020), https://perma.cc/9CKH-VE4T.

loom large. For contact tracing, such a scheme is only effective if combined with a broad and effective testing regime. Meanwhile, preemptive quarantine enforcement could act as a disincentive to the voluntary testing and full revelation of contacts demanded for contact tracing, given concerns about being subject to constant state monitoring.

There may, of course, be situations in which the perceived benefits outweigh these risks—if, for example, there is widespread failure to abide by quarantine orders and demonstrably negative health consequences as a result. Any such decision should fully incorporate a fair-minded assessment of both the benefits and the risks, looking at the program as a whole— and not just invoked in response to the kind of fear that often takes hold during a time of emergency.

Seventh, any program ultimately adopted should incorporate robust review and oversight. This is necessary to ensure that the program is satisfying the stated need. It is also necessary to assess the costs—to security of personal information, to privacy, and to other civil liberties.

Eighth, transparency. Unlike law enforcement or national security surveillance, which require secrecy as a component of effectiveness, health surveillance has the goals of educating and informing. Transparency is a key component of the trust that is needed to achieve the best outcomes possible.

Ninth, equity in both design and application. This requires clear criteria in terms of when, how, and according to what standards surveillance systems are put in place. It requires limits on discretionary application—as a means of protecting against arbitrariness and discrimination. And it requires consideration of how such surveillance programs may unduly impact already marginalized communities—as well as protections to avoid discriminatory effect.[95]

Not only are these recommendations good policy, they also are critical to the legal analysis, for all the reasons already discussed, as well.[96]

CONCLUSION

Good health and good privacy go hand in hand. Health surveillance is an inherent part of promoting good health. Technology can aid those efforts. But we should avoid being lulled into tech utopianism, without a clear-eyed consideration of both the benefits and risks. Such uses of technology should be done in ways that protect core liberties, and in doing, instill trust. This requires a careful assessment of need, tailoring of program to need, and consideration of the immediate and long-term implications of any new surveillance schemes set up.

---

95. *See, e.g.*, Susan Landau, Christy E. Lopez & Laura Moy, *The Importance of Equity in Contact Tracing*, LAWFARE (May 1, 2020, 3:15 PM), https://perma.cc/75VQ-4UU5. *See* Wendy K. Mariner et al., *Pandemic Preparedness: A Return to the Rule of Law*, 1 DREXEL L. REV. 341, 358–59 (2009) (warning that quarantine and health surveillance measures have historically had a disproportionate effect on already marginalized and disadvantaged communities); Rozenshtein, *Digital Disease Surveillance*, *supra* note 76, at 30-32.

96. *See also* Ram & Gray, *supra* note 50, at 16-25 (offering a thoughtful set of recommendations to guide legislators designing health surveillance systems); Rozenshtein, *Digital Disease Surveillance*, *supra* note 76, at 24-41.

Among the core questions, does the technology actually provide sufficiently reliable information to be useful? Are the data destroyed after the point at which they serve the health purpose for which they are collected? Mandatory contract tracing is more effective than voluntary contact tracing. But for what purpose and at what unintended costs? For all such programs, how are the data that are collected handled? Who holds the data? How securely are they being held? Who can access the data? And how long are they retained?

These are all questions that need to be asked and answered. They matter to our health. They matter to the law. They matter to the protection of our core liberties. And they matter to our post-COVID future as well.