LEAD ARTICLE

DIGITAL DISEASE SURVEILLANCE

ALAN Z. ROZENSHTEIN*

The fight against future pandemics will likely involve digital disease surveillance: the use of digital technology to enhance traditional public-health techniques like contact tracing, isolation, and quarantine. But legal scholarship on digital disease surveillance is still in its infancy. This Article fills that gap.

Part I explains the role that digital disease surveillance could have played in responding to coronavirus, and the role it likely will play in future infectious-disease outbreaks. Part II explains how the "special needs" exception to the Fourth Amendment's warrant requirement permits almost any rationally designed disease surveillance program. Part III suggests safeguards beyond what Fourth Amendment doctrine currently requires that could protect rights without diminishing surveillance effectiveness, including review for effectiveness and equality, procedural requirements, and periodic legislative authorization. Part IV proposes a mixed standard for judicial review: courts should require these safeguards under an evolving understanding of Fourth Amendment reasonableness

* Associate Professor of Law, *University of Minnesota Law School*. For helpful comments I thank Marc Blitz, Hannah Bloch-Wehba, Kiel Brennan-Marquez, Ryan Calo, Glenn Cohen, Aaron Cooper, Rebecca Crootof, Jen Daskal, Jolynn Dellinger, Scott Dewey, Mailyn Fidler, Richard Frase, Bob Gellman, Woody Hartzog, Claire Hill, Margaret Hu, Aziz Huq, Steve Koh, Bill McGeveran, Justin Murray, Maria Ponomarenko, Eve Brensike Primus, Shalev Roisman, Bruce Schneier, Scott Skinner-Thompson, Francis Shen, Christopher Slobogin, Matt Tokson, Mayank Varia, Lindsay Wiley, Ari Ezra Waldman, Andrew Woods, participants at the *University of Florida*'s National Security Junior Scholars Workshop, the *University of Minnesota Law School*'s summer workshop series, the *University of Nebraska*'s Law & Technology Virtual Workshop, and the *University of Oklahoma*'s Mini-Conference on Coronavirus and Law. For excellent research and editorial assistance, I thank Avery Bennett, Braxton Haake, Sarani Rangarajan Millican, Daniel Walsh, and the editors of the *American University Law Review*.

while tempering their review with deference to the political branches. Part IV concludes by outlining how the doctrinal evolution spurred by digital disease surveillance programs—the development of a "special needs with bite" standard—might advance a key research agenda in criminal procedure: how to apply the Fourth Amendment to modern, data-driven surveillance regimes.

TABLE OF CONTENTS

INTRODUCTION

Many governments have fought the coronavirus pandemic with *digital disease surveillance*, using digital technology, often in ways that overlap with law-enforcement surveillance, to enhance traditional public health techniques.[1] The United States—the world's richest and most technologically advanced country and the home of the leading technology giants—is a notable exception.[2]

There are many reasons for the United States' failure to use what could have been useful public health tools. During the Trump administration, the federal government exercised little meaningful leadership as to the pandemic response, instead leaving states on their own, one result of which was a fragmented landscape of state smartphone apps with relatively low public uptake.[3] Design choices by Apple and Google—in part responsive to broader privacy concerns among the public—limited the effectiveness of contact tracing apps built on their platforms.[4] And an early shortage of testing made contact tracing—whether digital or analog—less effective than it would have otherwise been.[5] These problems are all fixable, but at this point, with effective vaccines being widely administered, we will likely reach broad

---

1. *See* Niall McCarthy, *Which Countries Are Deploying Coronavirus Tracing Apps?*, FORBES (July 22, 2020, 6:02 AM), https://www.forbes.com/sites/niallmccarthy/2020/07/22/which-countries-are-deploying-coronavirus-tracing-apps-infographic/?sh=2ee1c7136d34 [https://perma.cc/CS39-7ELL] (stating that almost fifty countries either developed or implemented varying COVID-19 contact tracing apps); *see also* Jennifer Daskal, *Good Health and Good Privacy Go Hand-in-Hand*, 11 J. NAT'L SEC. L. & POL'Y, 131, 137–38 (2020).

2. *See* Alejandro de la Garza, *Contact Tracing Apps Were Big Tech's Best Idea for Fighting COVID-19. Why Haven't They Helped?*, TIME (Nov. 10, 2020, 7:00 AM), https://time.com/5905772/covid-19-contact-tracing-apps [https://perma.cc/BX8M-L9H9] (discussing the slow progress of contact tracing apps in the United States).

3. *See* Yasmeen Abutaleb et al., *The Inside Story of How Trump's Denial, Mismanagement and Magical Thinking Led to the Pandemic's Dark Winter*, WASH. POST (Dec. 19, 2020), https://www.washingtonpost.com/graphics/2020/politics/trump-covid-pandemic-dark-winter/ (detailing the Trump administration's shortcomings in responding to the COVID-19 pandemic including, among other things, failing to implore the use of masks and implement meaningful action on testing).

4. Jane Bambauer & Brian Ray, *COVID-19 Apps Are Terrible—They Didn't Have to Be*, LAWFARE 17–19 (Dec. 21, 2020, 8:01 AM), https://www.lawfareblog.com/covid-19-apps-are-terrible-they-didnt-have-be [https://perma.cc/G6N7-J3M7].

5. Aria Bendix, *The US's Contact-Tracing System Is Broken. Testing Delays Set It up for Failure*, BUS. INSIDER (Aug. 6, 2020, 8:13 AM), http://www.businessinsider.com/us-contact-tracing-coronavirus-failure-testing-delays-2020-8 [https://perma.cc/622S-L7SE].

immunity by the middle of 2021, with or without digital disease surveillance tools.[6]

But even if the United States ends up eschewing digital disease surveillance in its fight against coronavirus, it is still important to fully understand the options for and implications of such surveillance, because the next global pandemic may leave us with no choice. For all of coronavirus's devastating impacts, it could have been far worse: it is less than half as deadly as the 1918 flu, which was also particularly lethal for children and young adults, groups that are currently being spared the worst of coronavirus's effects.[7] In our interconnected world, the appearance of a disease as bad as (or even worse than) the 1918 flu is only a matter of time.[8] And if we are as unprepared when that happens as we were for coronavirus, concerns about the privacy or civil-liberties impacts of digital disease surveillance will likely be swept aside. The stakes are high: now is the time to design an effective digital-disease-surveillance program, one that protects health *and* civil liberties, before circumstances require us to slap something together quickly and no matter the costs.

Unfortunately, legal scholarship on government-led digital disease surveillance is still in its infancy. On the one hand, while the literature on the Fourth Amendment and government surveillance in general

---

6. Marisa Fernandez, *Fauci: U.S. Could Achieve Herd Immunity by Fall if Vaccine Rollout Goes to Plan*, AXIOS (Jan. 19, 2021), https://www.axios.com/fauci-us-achieve-herd-immunity-fall-vaccine-2992697d-3936-4960-89bc-be4977115bde.html [https://perma.cc/6V38-PCBE]; *see also* Robert Bollinger & Stuart Ray, *New Variants of Coronavirus: What You Should Know*, JOHNS HOPKINS MED. (Feb. 22, 2021), https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/a-new-strain-of-coronavirus-what-you-should-know [https://perma.cc/5DBV-MKQU].

7. *See* Jon Hamilton, *Antibody Tests Point to Lower Death Rate for the Coronavirus than First Thought*, NAT'L PUB. RADIO (May 28, 2020, 1:11 PM), https://www.npr.org/sections/health-shots/2020/05/28/863944333/antibody-tests-point-to-lower-death-rate-for-the-coronavirus-than-first-thought [https://perma.cc/7QMW-QH54] (adding that the best estimates for COVID-19 fatality rates are between 0.5% and 1%, which is less deadly than it initially appeared); Jeffrey K. Taubenberger & David M. Morens, *1918 Influenza: The Mother of All Pandemics*, 12 EMERGING INFECTIOUS DISEASES 15, 15 (2006) (stating that fatality rates for the 1918 influenza pandemic were greater than 2.5%).

8. Even as coronavirus rages, scientists are tracking other pandemic-capable diseases. *See* Mike Ives, *Scientists Say New Strain of Swine Flu Virus Is Spreading to Humans in China*, N.Y. TIMES (July 1, 2020), https://www.nytimes.com/2020/06/30/world/asia/h1n1-swine-flu-virus-china-pig.html (reporting on new strains of the H1N1 swine flu virus that must be "urgently" controlled given that they display "all the essential hallmarks of a candidate pandemic virus").

pays substantial attention to other forms of electronic surveillance, it has mostly ignored disease surveillance.[9] On the other hand, the privacy and health law scholarship on health information either focuses on the collection of such information by private parties,[10] or, when it comes to public health, largely passes over its Fourth Amendment implications.[11]

These gaps in the scholarship deprive policymakers of the information they need to optimize disease surveillance programs, which leaves courts unsure of how they should review such programs and makes it harder for the public to demand the best of its government. This Article seeks to fill this scholarly gap by making four contributions.

---

9. An important exception is Edward P. Richards's excellent *Dangerous People, Unsafe Conditions: The Constitutional Basis for Public Health Surveillance*, 30 J. LEGAL MED. 27 (2009), which argues that digital disease surveillance, even without warrants or probable cause, would generally be allowed by the Fourth Amendment "[a]s long as the state is acting to prevent future harm and not to punish the individual," *id.* at 28, a conclusion with which I broadly agree, *see infra* II.C. But Richards's analysis predated important developments in both technology—namely the proliferation of smartphones—and surveillance law and policy, including cases like *United States v. Jones*, 565 U.S. 400 (2012), *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the disclosure of mass government surveillance by Edward Snowden, and the consequent legislative reforms like the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

More recently, legal scholars have begun to explore the use of epidemiological surveillance to fight coronavirus. *See* Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID-19*, 7 J.L. & BIOSCIENCES 1, 1 (2020) (arguing, among other things, that the Fourth Amendment's protection against unreasonable searches and seizures may apply to location data used for epidemiological purposes, though the special needs doctrine may justify these potential searches and seizures); Emily Berman, Leah R. Fowler & Jessica L. Roberts, *COVID-19 Surveillance* (Aug. 5, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3666300.

10. Most of this scholarship focuses on HIPAA, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.), and its associated Privacy Rule, 45 C.F.R. pts. 160, 164.

11. For example, the leading work on public health law comprehensively discusses federalism, due process, and First Amendment limits on public-health programs. *See* LAWRENCE O. GOSTIN & LINDSAY F. WILEY, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 73–151 (3d ed. 2016). Discussion of the Fourth Amendment is largely limited to one district court case (understandably, since the kind of programmatic electronic surveillance discussed in this Article is a novel development). *See id.* at 322 (discussing Or. Prescription Drug Monitoring Program v. DEA, 998 F. Supp. 2d 957 (D. Or. 2014), *rev'd*, 860 F.3d 1228 (9th Cir. 2017)).

Part I argues that government-mandated disease surveillance could have played a useful role in fighting COVID-19, and likely will play such a role during future infectious-disease outbreaks.[12] Thus, whether one supports or opposes digital disease surveillance, it is imperative to analyze its legal and policy implications.

Part II explains how current Fourth Amendment doctrine—specifically the "special needs" (or "administrative search") exception to the warrant requirement—permits almost any rationally designed disease surveillance program, whether supported by individualized suspicion or not, as long as the surveillance is not primarily used for traditional law enforcement purposes.

Part III offers safeguards that go beyond what the Fourth Amendment requires and that could protect rights without diminishing surveillance effectiveness. Such safeguards include review for effectiveness and equality; use restrictions that limit how disease surveillance data is used; ex ante judicial authorization; internal procedures through public

---

12. This Article does not address disease surveillance undertaken by the private sector, which raises a host of legal and policy issues, including how to make sure that companies comply with non-discrimination and privacy laws, and whether companies should be restricted in their use of health data for non-public health purposes (e.g., advertising). *See, e.g.*, Matthew T. Bodie & Michael McMahon, *Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic*, 64 WASH. U. J.L. & POL'Y (2020) (manuscript at 1–2) (arguing that despite lacking federal guidance, private-sector employers can implement a responsible testing, tracing, and disclosure program provided they minimize invasions into worker privacy). For recent legislative proposals to this effect, *see* Rebecca Robbins, *Federal Legislation to Protect Health Data Has Made Little Progress. Will that Change in the Covid-19 Era?*, STAT (May 20, 2020), https://www.statnews.com/2020/05/20/health-data-patient-privacy-legislation-congress [https://perma.cc/6WEB-RVUN] (discussing three bills aiming to regulate health data related to coronavirus).

Admittedly, the line between the public and private sectors is an often blurry one. In particular, the government has, both throughout American history and in recent decades, expanded its power by partnering with private actors. *See, e.g.*, JON D. MICHAELS, CONSTITUTIONAL COUP: PRIVATIZATION'S THREAT TO THE AMERICAN REPUBLIC (2017); William J. Novak, *The Myth of the "Weak" American State*, 113 AM. HIST. REV. 752, 769–71 (2008) (stating that the public sector uses the private sector to accomplish public objectives); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1285 (2003) (suggesting that the trend toward privatization is not shrinking government but rather an "expan[sion of] government's reach into realms traditionally thought private"). No doubt digital disease surveillance could follow this pattern as well, with the federal and state governments partnering—either cooperatively or through legal mandates—with private actors to conduct disease surveillance.

rulemaking; oversight, transparency and public reporting; and periodic legislative authorization through sunset provisions.

Part IV addresses judicial review of digital disease surveillance programs. It argues that, in the long term, courts should require these safeguards under an evolving understanding of Fourth Amendment reasonableness, though they should temper this review with substantial deference to the political branches. It also outlines how doctrinal evolution, spurred by digital-disease-surveillance programs, might advance a key research agenda in criminal procedure: how to apply the Fourth Amendment to modern, data-driven surveillance regimes. Specifically, Fourth Amendment doctrine would benefit from what I call "special needs with bite": an alternate approach to warrantless searches that avoids both the rigidity of the traditional emphasis on probable cause and the overly permissive nature of the current special needs doctrine.

I. THE PROMISE OF DIGITAL DISEASE SURVEILLANCE

This section starts with an overview of the coronavirus pandemic. It then discusses the role that digital surveillance could have played in America's response to the pandemic, the limitations and dangers of such technology, and the political prospects for its adoption. It argues that, for good or ill, digital disease surveillance will be a pervasive part of the government's response to future pandemics.

To be clear, I am *not* making the normative argument that governments *should* aggressively use digital disease surveillance. Any judgment on the merits would depend on the course of a particular pandemic and the specific details of the surveillance program at issue. It is conceivable (though I believe unlikely) that digital disease surveillance is never the right option; even well-designed digital disease surveillance presents many dangers to privacy, liberty, and equality, and there is no guarantee that such surveillance will be well designed. (These dangers and how to address them are the topic of Part III). But I do argue that there is a strong prima facie case for taking digital disease surveillance seriously as a possible public health intervention.

I also recognize that people have strong and differing normative priors as to the relative importance of (and the appropriate risk tolerance for) the many values at stake, from privacy and equality to

public health and economic growth.[13] It is thus not surprising that leading scholars have come to dramatically different conclusions, for example, about the desirability of contact tracing apps.[14] I personally am sympathetic to digital disease surveillance, but nothing in this section (or the larger Article) requires that the reader share this view. I respect that, for many, the risks of increased surveillance will outweigh its potential benefits. But regardless of one's personal view as to the desirability of digital disease surveillance, it is likely to be part of the government response to future pandemics. For this reason alone, it is crucial to analyze both its legality as well as ways to improve it.

A. The Coronavirus Pandemic

Coronavirus disease 2019 (COVID-19) is caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), which, as of May 2021, has infected over-150 million people around the world, killing over three million.[15] In the United States, the official report is over 32 million infected and nearly 580,000 dead.[16] The actual death toll may be almost twice as high.[17] Although the vast majority of infections are

---

13. These are only some of the values implicated by the coronavirus pandemic. Indeed, it is difficult to think of a single important social issue that has not been affected, one way or another, by the disease. To highlight just one, coronavirus threatens voting rights, since people might be too scared to go to the polls or governments might reduce voting availability, or, in the worst-case scenario, try to postpone or even cancel elections. Thus, digital disease surveillance could help protect the right to vote. At the same time, the same surveillance authorities could be abused to harass potential voters. The devil stubbornly remains in the details.

14. *Compare* Jane Bambauer et al., *It's Time to Get Real About COVID Apps*, MEDIUM (May 14, 2020), https://medium.com/@DataVersusCovid/its-time-to-get-real-about-covid-apps-dd82e08895f2 [https://perma.cc/AYL4-LNL5] (arguing for the use of contact tracing apps), *with* Ashkan Soltani et al., *Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis*, BROOKINGS (Apr. 27, 2020), https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster [https://perma.cc/CP72-7V8F] (arguing against).

15. *Weekly Epidemiological Update—11 May 2021*, WORLD HEALTH ORG. (May 11, 2021), https://www.who.int/publications/m/item/weekly-epidemiological-update-on-covid-19—11-may-2021 [https://perma.cc/X6SN-DPDV].

16. *Id.*

17. *Estimation of Total Mortality Due to COVID-19*, INST. FOR HEALTH METRICS & EVALUATION tbl.1 (May 6, 2021), http://www.healthdata.org/special-analysis/estimation-excess-mortality-due-covid-19-and-scalars-reported-covid-19-deaths [https://perma.cc/JRX5-RZLN] (estimating the total number of U.S. COVID-19 deaths at over 900,000); Josh Katz et al., *U.S. Coronavirus Death Toll Is Far Higher than*

not fatal, serious complications include severe lung damage,[18] blood-clotting disorders,[19] brain disorders,[20] and, in the case of children, the rare but serious Kawasaki-like disease.[21]

To limit the spread of the disease, states imposed unprecedented lockdowns, closing businesses and keeping hundreds of millions of people at home.[22] While necessary to slow the spread of the virus, the upending of economic and social life has been severe. Unemployment reached nearly fifteen percent in the spring of 2020 and could remain elevated for years to come.[23] In 2020, gross domestic product (GDP) fell by as much as thirty percent annualized.[24] These economic effects, bad enough alone as they are, have imposed enormous second-order harms on mental and physical health.[25] In addition, confining people at home increases rates of domestic violence[26] and, to the extent that it prevents people from accessing healthcare, non-coronavirus illnesses

---

Reported, C.D.C. Data Suggests, N.Y. TIMES (Apr. 28, 2020), https://www.nytimes.com/interactive/2020/04/28/us/coronavirus-death-toll-total.html.

18. Yuhui Wang et al., *Temporal Changes of CT Findings in 90 Patients with COVID-19 Pneumonia: A Longitudinal Study*, 296 RADIOLOGY 6 (2020).

19. Jean M. Connors & Jerrold H. Levy, *COVID-19 and Its Implications for Thrombosis and Anticoagulation*, 135 BLOOD PERSP. 2033, 2034 (2020).

20. Ross W. Paterson et al., *The Emerging Spectrum of COVID-19 Neurology: Clinical, Radiological and Laboratory Findings*, 143 BRAIN 3104, 3104 (2020).

21. Russell M. Viner & Elizabeth Whittaker, *Kawasaki-Like Disease: Emerging Complication During the COVID-19 Pandemic*, 395 LANCET 1741, 1741–42 (2020).

22. *See Coronavirus Restrictions and Mask Mandates for All 50 States*, N.Y. TIMES (Feb. 12, 2021), https://www.nytimes.com/interactive/2020/us/states-reopen-map-coronavirus.html.

23. Jeanna Smialek, *Fed Leaves Rates Unchanged and Projects Years of High Unemployment*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/business/economy/federal-reserve-economy-coronavirus.html.

24. Jeanna Smialek, *Fed Chair Says Economic Recovery May 'Stretch' Through End of 2021*, N.Y. TIMES (May 17, 2020), https://www.nytimes.com/2020/05/17/business/economy/fed-powell-economic-recovery.html.

25. *See* M.B. Pell & Benjamin Lesser, *Researchers Warn the COVID-19 Lockdown Will Take Its Own Toll on Health*, REUTERS (Apr. 3, 2020, 12:00 PM), https://www.reuters.com/investigates/special-report/health-coronavirus-usa-cost [https://perma.cc/Z7JS-A6HE] (citing reports that COVID-19 shutdowns have increased domestic violence, school dropouts, and suicides, while decreasing health services and employment).

26. *See* Amanda Taub, *A New COVID-19 Crisis: Domestic Abuse Rises Worldwide*, N.Y. TIMES (Apr. 6, 2020), https://www.nytimes.com/2020/04/06/world/coronavirus-domestic-violence.html (reporting that movement restrictions may be "making violence in homes more frequent, more severe and more dangerous").

and death.[27] In short, COVID-19 has caused a level of social and economic devastation unseen since the Great Depression.[28]

Fortunately, the development and administration of effective vaccines could lead to the end of the pandemic sometime in the second half of 2021.[29] But no matter how quickly the pandemic ends, it will have wrought enormous damage. It is thus important to analyze what role digital disease surveillance could have played in the fight against COVID-19.

B. Digital Surveillance to Fight Disease

The term "disease surveillance," as it is used by public health professionals, refers to the "ongoing, systematic collection, analysis, and interpretation of health data used in the planning, implementation, and evaluation of public health programs."[30] Disease surveillance is different from (though it serves as a key input to) nonpharmaceutical interventions like contact tracing, quarantine, and isolation.[31] And "digital disease surveillance," under this definition, could refer to any use of information technology to facilitate digital surveillance, from digital communications that collect health information to electronic databases that organize and process it. The increasing power and sophistication of this kind of

---

27. *See* Sam Williams et al., *An Improved Measure of Deaths Due to COVID-19 in England and Wales* 6 (Working Paper, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3635548 (noting the examples of England and Wales, in which "analysis suggests that the UK's lockdown has had a net positive impact on mortalities. That is to say, it resulted in more, not less, deaths. Intuitively, this may be due to the unintended consequences of the lockdown (for example, a substantial reduction in the provision of, or access to, other forms of critical healthcare) dominating its intended consequences.").

28. Gita Gopinath, *The Great Lockdown: Worst Economic Downturn Since the Great Depression*, IMFBLOG (Apr. 14, 2020), https://blogs.imf.org/2020/04/14/the-great-lockdown-worst-economic-downturn-since-the-great-depression [https://perma.cc/L9GE-NJZF].

29. *See* Tim Loh, *Fauci Says End to Pandemic Is in Sight, Thanks to Vaccines*, BLOOMBERG (Nov. 12, 2020, 11:48 AM), https://www.bloomberg.com/news/articles/2020-11-12/covid-won-t-be-pandemic-for-long-thanks-to-vaccines-fauci-says (claiming that with effective vaccines, the end is now in sight and the pandemic will not be around "for a lot longer").

30. Terence L. Chorba, *Disease Surveillance*, *in* EPIDEMIOLOGIC METHODS FOR THE STUDY OF INFECTIOUS DISEASES 138 (James C. Thomas & David J. Weber eds., 2001).

31. *See* de la Garza, *supra* note 2 (explaining that digital surveillance apps augment traditional contact tracing by alerting users to take subsequent actions like getting tested).

disease surveillance has been underway for decades and will no doubt continue.[32] Recent innovations, though considerable,[33] represent an evolutionary, rather than revolutionary, step, and raise the same legal and policy issues that public health and privacy law scholars have long studied.[34]

For this reason, in this Article I define *digital disease surveillance* more narrowly, as the use of digital (or "electronic")[35] surveillance to track the health status, contacts, and movement of individuals for the purpose of preventing disease. Unlike group-based surveillance, digital disease

---

32. *See* Stephen B. Thacker et al., *Public Health Surveillance in the United States: Evolution and Challenges*, 61 MORBIDITY & MORTALITY WKLY. REP. 3, 3–4 (2012) (recounting the history of healthcare surveillance in the United States starting in 1741).

33. The private sector has been particularly innovative. An early example is Google Flu Trends, which used user search queries to predict (though not very successfully) influenza spread. *See* David Lazer & Ryan Kennedy, *What We Can Learn from the Epic Failure of Google Flu Trends*, WIRED (Oct. 1, 2015, 7:00 AM), https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends [https://perma.cc/55H4-CXSJ] (documenting how Google's attempt to use search data to track influenza failed). More recently, population-level digital surveillance has been used to track coronavirus. For example, both Apple and Google are publicly sharing "mobility reports," which use aggregate anonymized data from smartphone users to show trends in whether populations are adhering to social-distancing guidelines. *Mobility Trends Reports*, APPLE, https://www.apple.com/covid19/mobility [https://perma.cc/T3JK-DV84]; *COVID-19 Community Mobility Reports*, GOOGLE, https://www.google.com/covid19/mobility [https://perma.cc/YUD2-8JNS]. And Kinsa, a maker of internet-connected thermometers, has used this information to predict new coronavirus hotspots. *See Kinsa's Atypical Illness Signal Is a Leading Indicator of COVID-19 Outbreaks*, KINSA (May 5, 2020), https://www.kinsahealth.co/kinsas-illness-signal-a-leading-indicator-covid-19-outbreaks [https://perma.cc/43K2-FPR9] (claiming that its "syndromic fever monitoring data" identified the onset of the COVID-19 pandemic in certain geographic areas before official reports).

34. Disease surveillance has always raised privacy concerns. The problem that information technology poses is one of increased scale: "As vastly greater quantities of data are collected, integrated, and transmitted to a growing number of users, the ability of individuals to control access to personal information is sharply reduced." GOSTIN & WILEY, *supra* note 11, at 307. This has exacerbated what the Supreme Court has recognized as the "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." Whalen v. Roe, 429 U.S. 589, 605 (1977).

35. *See generally* JAMES G. CARR ET AL., 1 LAW OF ELEC. SURVEILLANCE § 1:1 (2020) (defining electronic surveillance as "the acquisition of communications and related information through techniques that traditionally have involved use of electronic or other mechanical devices").

surveillance tracks people as individuals (rather than anonymizing and aggregating information) and targets public health interventions accordingly.[36] This definition highlights the novelty of using widespread electronic surveillance for public health purposes and the new legal and policy issues such surveillance raises. And within this category, this Article focuses on the most likely uses for digital disease surveillance in the immediate future: (1) contact tracing and (2) tracking to enforce isolation and quarantine.[37]

As traditionally practiced, contact tracing involves asking infected individuals for a list of people with whom they came into close contact for some minimum period of time over some duration (often with a focus on identifying clusters and super-spreader events).[38] Those individuals are then tested and in turn asked for their contacts, and so on.[39] In this way, an infection can be tracked through a population and, with appropriate treatment, quarantine, and isolation, controlled.

Digital contact tracing systems differ across several dimensions. One dimension is whether the data that is collected and analyzed is stored centrally by the government or instead is decentralized across user devices.[40] Centralized systems raise additional privacy concerns and thus have seen greatest adoption in authoritarian countries, most

---

36. *See, e.g.*, Brian Kim, *Lessons for America: How South Korean Authorities Used Law to Fight the Coronavirus*, LAWFARE (Mar. 16, 2020, 2:39 PM), http://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus [https://perma.cc/AR7Y-APJV] (reporting that South Korea's COVID-19 tracking app provided individual details as granular as which theater seats individuals sat in).

37. There are of course many other potential forms of digital disease surveillance. Facial recognition could be used to identify individuals that have attended known super-spreader events. Analysis of internet behavior—for example, search-engine queries or social-media posts—could identify symptomatic individuals. Because contact tracing and location monitoring are the most popular digital disease surveillance techniques being used in the United States and around the globe, this Article uses them to analyze the broader legal and policy issues around digital disease surveillance.

38. William F. Marshall, III, *Contact Tracing and COVID-19: What Is It and How Does It Work?*, MAYO CLINIC (Dec. 15, 2020), https://www.mayoclinic.org/diseases-conditions/coronavirus/expert-answers/covid-19-contact-tracing/faq-20488330 [https://perma.cc/JG82-VA7K].

39. *Id.*

40. *See* Cristina Criddle & Leo Kelion, *Coronavirus Contact-Tracing: World Split Between Two Types of App*, BBC (May 7, 2020), https://www.bbc.com/news/technology-52355028 [https://perma.cc/J8A7-3VXH] (describing how centralized and decentralized tracking apps work).

notably China, which used centralized digital disease surveillance to great effect.[41] But several liberal democracies, notably South Korea[42] and France,[43] have pursued centralized approaches.[44] Still, decentralized systems are proving more popular among liberal democracies.[45] The most popular decentralized protocol is Apple and Google's jointly developed Privacy-Preserving Contact Tracing system,[46] which has become the major platform on which states are building their own contact tracing apps.[47]

Systems also differ based on the kind of data they collect, and how. Some systems, like South Korea's, use a variety of collection mechanisms to track people's movements and contacts, including "location data (including location data collected from mobile devices); personal identification information; medical and prescription records; immigration records; card transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and closed-circuit television (CCTV)

41. *See* Raymond Zhong, *China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears*, N.Y. TIMES (May 26, 2020), https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html (discussing concerns that coronavirus monitoring apps that China developed may continue to be a permanent part of everyday life, in which authorities have taken "an expansive view of using high-tech surveillance tools in the name of public well-being").

42. *See* Kim, *supra* note 36 (describing the South Korean government's legislative actions authorizing its centralized approach to digital disease surveillance).

43. *See* Leo Kelion, *Coronavirus: France's Virus-Tracing App 'Off to a Good Start'*, BBC (June 3, 2020), https://www.bbc.com/news/technology-52905448 [https://perma.cc/2QH3-D5GH] (describing France's implementation of a centralized approach in opposition to academics' concerns about repurposing collected data for mass surveillance).

44. *See* Criddle & Kelion, *supra* note 40 (pointing out Australia, Norway, and India as adopters of centralized approaches).

45. *See id.* (noting a list of countries, including Germany, Italy, Switzerland, Latvia, Austria, Estonia, Finland, Ireland, and Canada, which favor decentralization).

46. Press Release, Apple, Apple and Google Partner on COVID-19 Contact Tracing Technology (Apr. 10, 2020), https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology [https://perma.cc/MT8D-K4J3]; *Privacy-Preserving Contact Tracing*, APPLE, https://covid19.apple.com/contacttracing [https://perma.cc/9ZYL-6DM6].

47. *See* Lindsey Van Ness, *For States' COVID Contact Tracing Apps, Privacy Tops Utility*, PEW CHARITABLE TR. (Mar. 19, 2021), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/19/for-states-covid-contact-tracing-apps-privacy-tops-utility [https://perma.cc/QL9C-263C] (reporting that twenty-four states and Washington, D.C. are using Apple and Google's systems with the expectation of more collaborations).

footage."[48] Other systems use only location data provided by a person's smartphone, either through low-range Bluetooth radio signals or GPS.[49] Each of these technologies has its own benefits and tradeoffs. GPS, for instance, identifies actual location but does not work well inside buildings.[50] By contrast, Bluetooth (which is at the heart of the Apple-Google and other popular proposals) works inside structures and can potentially more precisely identify when two individuals have come into contact, but it does not identify where the meeting took place.[51]

Whatever the implementation details, digital technology holds out the promise of mitigating two problems with the traditional, "analog" contact tracing.[52] First, traditional contact tracing takes an enormous amount of resources, especially in terms of the number of skilled contact tracers that are necessary in a large population.[53] This corps of

---

48. Sangchul Park et al., *Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies*, 323 JAMA 2129, 2129 (2020); *see also* Max S. Kim, *Seoul's Radical Experiment in Digital Contact Tracing*, NEW YORKER (Apr. 17, 2020), https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing [https://perma.cc/ZK6Z-AKT8] (detailing the South Korean government's transparency in sharing collected information, including routes of individuals testing positive for COVID-19); Dylan Scott & Jun Michael Park, *South Korea's Covid-19 Success Story Started with Failure*, VOX (Apr. 19, 2021, 7:00 AM), https://www.vox.com/22380161/south-korea-covid-19-coronavirus-pandemic-contact-tracing-testing (describing South Korean legal mandates that enable the government to obtain "financial or location data" for disease surveillance).

49. Thorin Klosowski, *COVID Contact Tracing Apps Are Far from Perfect*, N.Y. TIMES (Nov. 2, 2020), http://www.nytimes.com/wirecutter/blog/covid-contact-tracing-apps.

50. JAY STANLEY & JENNIFER STISA GRANICK, ACLU, THE LIMITS OF LOCATION TRACKING IN AN EPIDEMIC 3 (2020).

51. *See* Klosowski, *supra* note 49 (explaining that Google and Apple's software uses Bluetooth to capture only geographic proximity between devices).

52. Initial results from newly formed analog contact tracing programs, such as in New York City, are mixed. *See* Sharon Otterman, *N.Y.C. Hired 3,000 Workers for Contact Tracing. It's off to a Slow Start*, N.Y. TIMES (June 21, 2020), https://www.nytimes.com/2020/06/21/nyregion/nyc-contact-tracing.html (reporting that in the program's first two weeks, the city's 3,000 contact tracers were only able to obtain close contact information from 35% of the 5,347 residents who tested positive for COVID-19 or were presumed positive).

53. *See* Tanya Albert Henry, *Experts: Here's How Many More Contact Tracers U.S. Needs*, AM. MED. ASS'N (July 30, 2020), https://www.ama-assn.org/delivering-care/public-health/experts-here-s-how-many-more-contact-tracers-us-needs [https://perma.cc/25WL-4F8D] (stating that experts believed the United States

public health professionals is not only expensive to maintain and operate but is difficult to staff, given the required skills and training.[54]

Second, traditional contact tracing requires infected individuals to answer accurately about their past contacts.[55] But even if individuals decide to be truthful (which is not guaranteed[56]), memories are fallible, and people may not know the names of the people they interacted with, especially in anonymous public spaces.[57] Moreover, coronavirus exacerbates both of these problems because of the prevalence of asymptomatic infection.[58] A large proportion of infected individuals—especially those who are young and otherwise in good health—will exhibit no symptoms, either in the early stages of the disease or at all.[59] This group may be particularly unwilling to self-isolate, thus increasing the burden on public health agencies.[60] As a

---

needed over 100,000 additional contact tracers and more funding to control the transmission of COVID-19).

54. *Training Case Investigators and Contract Tracers*, CDC (Jan. 26, 2021), https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/training-investigators.html [https://perma.cc/72RJ-8635].

55. *See* Jaclyn Diaz, *Australian State Cuts COVID Lockdown Short, Saying Man Lied to Contact Tracers*, NAT'L PUB. RADIO (Nov. 20, 2020, 4:03 AM), https://www.npr.org/sections/coronavirus-live-updates/2020/11/20/936957351/australian-state-cuts-covid-lockdown-short-saying-man-lied-to-contact-tracers [https://perma.cc/R5AW-P8WG] (reporting that one individual lying to contact tracers triggered a strict lockdown in South Australia).

56. *See, e.g.*, Ed Shanahan, *Party Guests Won't Talk After 9 Tested Positive. Then Subpoenas Came*, N.Y. TIMES (Aug. 7, 2020), https://www.nytimes.com/2020/07/01/nyregion/rockland-coronavirus-party.html (reporting that county officials issued subpoenas after partygoers refused to speak with contact tracers and denied attending a party they in fact attended).

57. *See* Dyani Lewis, *Why Many Countries Failed at COVID Contact-Tracing—But Some Got It Right*, NATURE (Dec. 17, 2020), https://www.nature.com/articles/d41586-020-03518-4 [https://perma.cc/EWN7-5YRB] (writing that close contacts are of special interest to contact tracers and can include anyone who shared public transportation or office space with an infected individual).

58. Andrew A. Sayampanathan et al., *Infectivity of Asymptomatic Versus Symptomatic COVID-19*, 397 LANCET 93, 94 (2021).

59. *See Scientific Brief: Community Use of Cloth Masks to Control the Spread of SARS-CoV-2*, CDC (Nov. 20, 2020), https://www.cdc.gov/coronavirus/2019-ncov/more/masking-science-sars-cov2.html [https://perma.cc/KXW4-63EV] (estimating that asymptomatic or pre-symptomatic individuals account for more than fifty percent of transmissions).

60. *See* Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, 368 SCI. 1, 6 (2020) (stating that isolating

group of Oxford University researchers argued, "[t]raditional manual contact-tracing procedures are not fast enough for" the coronavirus.[61] They thus recommended the widespread use of contact tracing apps.[62]

Digital surveillance can also help enforce quarantine, the separation of individuals who have come in contact with an infected individual until they are determined to be free from disease, and isolation, the separation of individuals who are sick from those who are not.[63] The government could use location data (for example, cell-site location information held by mobile providers or GPS location data held by technology companies) to ensure that restricted individuals are staying in their homes or away from public spaces.[64] This may be particularly important for asymptomatic carriers (especially young people), who might be less willing to isolate for weeks on end if they are not feeling sick.[65]

It is important not to overstate the case for digital surveillance. Implementation would require overcoming both logistical and technical hurdles,[66] and the collection and centralization of so much

---

symptomatic individuals is insufficient as transmission of COVID-19 often occurs before individuals exhibit symptoms).

61. *Id.* at 1, 4.

62. *Id.* at 4.

63. Already one judge in Kentucky has ordered infected individuals who refuse to stay at home to wear location-monitoring electronic ankle bracelets. *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://www.reuters.com/article/us-health-coronavirus-quarantine-tech/to-keep-covid-19-patients-home-some-us-states-weigh-house-arrest-tech-idUSKBN22J1U8 (discussing states considering and implementing electronic surveillance measures to track infected individuals). Cell-phone-based surveillance could serve as a less-intrusive replacement (or adjunct) to such tracking. *Id.*

64. Asiyah Sheikh et al., *Novel Approaches to Estimate Compliance with Lockdown Measures in the COVID-19 Pandemic*, 10 J. GLOB. HEALTH 1 (2020).

65. There are many additional uses for digital technology in fighting infectious disease, such as "immunity passports" that would prove an individual's immune status and could be used as part of a regime that limits access to travel or employment to provably immune individuals. *See* Alexandra L. Phelan, *COVID-19 Immunity Passports and Vaccination Certificates: Scientific, Equitable, and Legal Challenges*, 395 LANCET 1595, 1596 (2020) (discussing problems pertaining to immunity passports, including their potential for abuse, implicit bias, and absence of evidence that people cannot contract COVID-19 more than once). Many of the policy considerations raised in Part III are relevant to such programs.

66. *See, e.g.*, STANLEY & GRANICK, *supra* note 50, at 2 (noting key questions to answer before using cell phone location data, including what data is used and who has access to the data); Susan Landau, *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, LAWFARE (Mar. 25, 2020, 10:46 AM), https://www.lawfareblog.com/location-

sensitive data raises obvious privacy and security concerns.[67] Moreover, a poorly designed surveillance program can be worse for public health than no surveillance at all, if it discourages individual compliance with public health measures. Even the best surveillance program should only be a complement, not a substitute, for traditional public health interventions, and it would be a serious failing if policymakers use digital surveillance as an excuse to underinvest in testing and treatment,[68] or push contact tracing to the point of diminishing marginal returns.[69] Finally, as with all public policy in our unequal society, there is a danger that digital disease surveillance will just perpetuate the Matthew effect:[70] the benefits will accrue to those already well-situated to deal with a public health crisis, while the costs

---

surveillance-counter-covid-19-efficacy-what-matters [https://perma.cc/R8AN-JZTT] (emphasizing the importance of efficient phone tracking if the technology will be useful); Bruce Schneier, *Me on COVID-19 Contact Tracing Apps*, SCHNEIER ON SEC. (May 1, 2020, 6:22 AM), https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html [https://perma.cc/MAG4-RXGH] (criticizing contact tracing apps for the risks of false positives and false negatives and not informing individuals if they have been infected); Ashkan Soltani et al., *supra* note 14 (identifying the "host of pitfalls for voluntary, self-reported coronavirus apps," including risks of false positives and false negatives).

67. Even countries generally considered the most sophisticated when it comes to digital disease surveillance are dealing with security issues. *See* Choe Sang-Hun et al., *Major Security Flaws Found in South Korea Quarantine App*, N.Y. TIMES (July 28, 2020), https://www.nytimes.com/2020/07/21/technology/korea-coronavirus-app-security.html (reporting on the "serious security flaws that made private information vulnerable to hackers" in a South Korean quarantine app).

68. *See* I Glenn Cohen et al., *Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension*, 323 JAMA 2371, 2371 (2020) (showing that states such as Maryland, Massachusetts, and New York had the most successful strategies by "massively scaling up manual tracing" and using smartphone technologies to augment the manual tracing).

69. *See* Benjamin Armbruster & Margaret L. Brandeau, *Contact Tracing to Control Infectious Disease: When Enough Is Enough*, 10 HEALTH CARE MGMT. SCI. 341, 342 (2007) (carrying out a simulation model to demonstrate that "incremental investments in contact tracing yield diminishing reductions in disease prevalence").

70. "For unto every one that hath shall be given, and he shall have abundance: but from him that hath not shall be taken away even that which he hath." *Matthew* 25:29 (King James). Sociologist Robert Merton coined the "Matthew effect." *See* Robert K. Merton, *The Matthew Effect in Science*, 159 SCI. 56, 62 (1968) (discussing the expansion of the "Matthew effect" beyond just the "enhancement of the position of already eminent scientists who are given disproportionate credit" to an effect on communication systems that "reduce[s] the visibility of contributions by authors who are less well known").

will fall disproportionality on the disadvantaged, like the poor, the elderly, and minorities.[71]

At the same time, digital disease surveillance illustrates the maxim that the perfect should not be allowed to become the enemy of the good. A program need not be 100% effective to still make a substantial contribution to public health. Although digital contact tracing will not work for the roughly 20% of Americans who do not own a smartphone,[72] if it can change the behavior of or provide information on the 80% of Americans who do carry smart phones, that will make a substantial impact.[73] Similarly, although location-based quarantine/isolation enforcement might not work if people leave their phones at home, enough people might still be deterred from leaving their homes so as to make the program effective.

Importantly, the exponential nature of infection means that even interventions that have small changes on individual behavior can lead to large downstream public health benefits. Unfortunately, psychological and economic research has demonstrated the pervasiveness of the tendency to underestimate exponential growth.[74] This bias no doubt played a role in America's slow initial response to coronavirus.[75]

---

71. *See infra* Section III.A.2 (discussing equality, or lack thereof, in the outcomes of digital disease surveillance).

72. *Mobile Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/JP64-NFYW].

73. *Id.*

74. *See* David Robson, *Exponential Growth Bias: The Numerical Error Behind Covid-19*, BBC (Aug. 12, 2020), https://www.bbc.com/future/article/20200812-exponential-growth-bias-the-numerical-error-behind-covid-19 [https://perma.cc/B4UB-RWG4] (showing how "people consistently underestimate how fast [exponential] value increases" and how this bias affects how people understand the spread of COVID-19, while those "who are susceptible to the exponential growth bias are less concerned about Covid-19's spread, and less likely to endorse measures like social distancing, handwashing or mask wearing").

75. Even something as simple as whether to show the exponential growth of coronavirus cases as a straight line (using a log scale) or an exponential curve (using a linear scale), can affect how people perceive the pandemic, with log-scale graphs leading to less accurate perceptions. Alessandro Romano et al., *The Scale of COVID-19 Graphs Affects Understanding, Attitudes, and Policy Preferences*, 29 HEALTH ECONS. 1482, 1484 (2020).

C. The Politics of Digital Disease Surveillance

Just because a digital disease surveillance program is effective does not mean that it is politically feasible. As the stalled rollout of COVID-19 tracking programs demonstrates,[76] the political and institutional headwinds are not trivial.

First, as the controversy over the COVID-19 lockdowns shows, a sizeable portion of the population is resistant to strong government action to fight infectious disease. Indeed, many have refused to engage in even basic social-distancing precautions like wearing masks.[77]

Second, skepticism of government surveillance is pervasive across the political spectrum. For liberals and libertarians, the rise of the surveillance state after 9/11, and especially the 2013 Snowden disclosures, cautions against embracing yet more government surveillance.[78] Conservatives, who have traditionally been more comfortable with greater surveillance powers, have their own reasons to oppose its increase, including controversy over government surveillance of associates of the 2016 Trump campaign.[79]

Third, comprehensive national digital disease surveillance would require federal leadership, which, as the Trump administration demonstrated, cannot be taken for granted. Even with a White House

---

76. *See, e.g.*, Chas Kissick et al., *What Ever Happened to Digital Contact Tracing?*, LAWFARE (July 21, 2020, 1:36 PM), https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing [https://perma.cc/C8GM-JSAV] (showing slow rollouts of contact tracing apps or codes throughout the United States and in other countries like France, Canada, and Ghana); Jonathan Zittrain, *Is Digital Contact Tracing over Before It Began?*, MEDIUM (June 25, 2020), https://medium.com/berkman-klein-center/is-digital-contact-tracing-over-before-it-began-925c72036ee7 [https://perma.cc/2S2H-VV3D] (noting the general public's belief that the disease has been sufficiently managed and therefore less of the public feels it is necessary to use contact tracing apps).

77. Teo Armus, *"Sorry, No Mask Allowed": Some Businesses Pledge to Keep out Customers Who Cover Their Faces*, WASH. POST (May 28, 2020, 7:11 AM), https://www.washingtonpost.com/nation/2020/05/28/masks-not-allowed-coronavirus.

78. *See* Taewoo Nam, *Does Ideology Matter for Surveillance Concerns?*, 34 TELEMATICS & INFORMATICS 1572, 1576 (2017) ("Libertarians-liberals [have] a higher level of surveillance concerns than conservatives-communitarians.").

79. *See* Eric Tucker, *Barr Tightens Rules on Surveillance of Political Candidates*, AP NEWS (Sept. 1, 2020), https://apnews.com/article/ap-top-news-politics-us-news-8f2b8809c8e7029884b56143cdb06fb6 [https://perma.cc/4Z9V-WNQX] (showing how new restrictions were implemented before the 2020 elections to create "additional hurdles before pursing the same type of surveillance as was conducted . . . on a former adviser to Trump's 2016 campaign").

that wants to play an active role in public health, a frequently gridlocked Congress cannot be counted on to enact necessary legislation. There is even a question as to the federal government's legal authority to implement certain forms of digital disease surveillance. For example, if Congress lacks power under the Commerce Clause to mandate that Americans buy health insurance,[80] can it really require them to install contact tracing smartphone apps?

Nevertheless, in the medium-to-long term, digital disease surveillance may still prove to be more attractive than the main alternative, lockdowns.[81] First, lockdowns may not be a viable strategy going forward. Having experienced the economic and social costs of lockdown, Americans (and their politicians) are unlikely to want to repeat the experience.[82]

Second, because of its passive nature, surveillance is much less salient, and thus is less likely to provoke opposition, than are lockdowns. Contact tracing apps and cellphone-based monitoring programs can work in the background, only alerting users when action is needed.

---

80. *See* NFIB v. Sebelius, 567 U.S. 519, 561 (2012) ("[T]he Commerce Clause does not support the individual mandate.").

81. Of course, as the success of the COVID-19 vaccines shows, the best way to defeat an infectious disease is through the rapid development of a vaccine. But we cannot assume that future infectious diseases will be as amenable to rapid vaccine development as COVID-19 was. And even a rapidly developed vaccine would take months to develop and administer. *Vaccine and Research Development: How can COVID-19 Vaccine Development Be Done Quickly and Safely?*, JOHNS HOPKINS: CORONAVIRUS RSCH. CTR., https://coronavirus.jhu.edu/vaccines/timeline [https://perma.cc/KN5R-AVRP]. It is precisely in the initial months of an epidemic, before broad community transmission has made contact tracing useless, that digital disease surveillance would be most helpful.

82. *See, e.g.*, Alice Miranda Ollstein & Dan Goldberg, *Quarantine Fatigue: Governors Reject New Lockdowns as Virus Cases Spike*, POLITICO (June 10, 2020, 7:55 PM), https://www.politico.com/news/2020/06/10/quarantine-governors-lockdowns-coronavirus-312146 [https://perma.cc/HS5M-77JL] (showing that even in places with rising cases of coronavirus infections, there was political and public resistance to another shutdown). School closures have been particularly difficult for children and parents alike. It is thus unsurprising that some schools included digital contact tracing as part of their reopening plans. *See* Will Knight, *Schools Turn to Surveillance Tech to Prevent Covid-19 Spread*, WIRED (June 5, 2020, 7:00 AM), https://www.wired.com/story/schools-surveillance-tech-prevent-covid-19-spread [https://perma.cc/3MQ8-CYA4] (reporting a plan to require Ohio students to wear electronic beacons to track their locations, which would "log[] which students and teachers are in each classroom throughout the day").

And, in the case of contact tracing apps, if they are loaded and enabled by default, they do not require the user to do anything to participate.[83] Of course, follow-up action by the government based on this surveillance (e.g., enforced quarantine or isolation) could spur resistance, but even here it would apply to substantially fewer people than blanket lockdowns.

Third, digital disease surveillance programs can do good even when operated on a state-by-state level, even if a nationally coordinated approach would be more effective. Unlike the federal government, which is one of enumerated powers, states possess a general "police power" to act for the health safety of their populations (though of course states have to abide by other constitutional limitations, including the Fourth Amendment).[84] And unlike the federal government, many states have proven to be highly energetic and effective in responding to coronavirus.[85] While the federal government dithered throughout 2020, states across the political spectrum imposed massive policy interventions to keep their residents safe. If a state has the political and institutional capacity to lock millions of people in their homes for months on end, it can, if properly motivated, set up a far less intrusive program of digital disease surveillance.

As a kind of compromise position, some have argued that any digital disease surveillance program should be voluntary, to respect peoples' wishes not to be tracked or not to know their own disease status. For example, the Apple-Google smartphone contact tracing protocol requires explicit user opt-in.[86] And many legislators seem to agree that

---

83. Users generally do not change default settings on their applications and services. Charles Arthur, *Why the Default Settings on Your Device Should Be Right First Time*, GUARDIAN (Dec. 1, 2013, 3:00 PM), https://www.theguardian.com/technology/2013/dec/01/default-settings-change-phones-computers.

84. *See* Katherine Drabiak, *Disentangling Dicta:* Prince v. Massachusetts*, Police Power and Childhood Vaccine Policy*, 29 ANNALS HEALTH L. & LIFE SCIS. 173, 177, 208 (2020) (showing that "[u]nder the concept of police power, states have a duty to enact laws that promote the health, safety, and welfare of its residents," although "police power may not unduly impinge upon Constitutional rights").

85. *See* Tucker Doherty et al., *Which States Had the Best Pandemic Response?*, POLITICO (Oct. 15, 2020, 4:05 PM), https://www.politico.com/news/2020/10/14/best-state-responses-to-pandemic-429376 (highlighting the efforts of states across the country that were leaders in responding to COVID-19, including Vermont, Washington, Michigan, Colorado, Iowa, Minnesota, Massachusetts, Connecticut, Rhode Island, and Florida, and the varied methods they employed that were successful).

86. Press Release, Apple, *supra* note 46.

user opt-in should be a precondition of digital disease surveillance.[87] Coronavirus data-privacy bills introduced by Democratic and Republican senators—both of which require affirmative consent before private entities (and in some cases government agencies) can use coronavirus-related data for disease tracking—suggest an emerging bipartisan consensus.[88]

But in the long term, policymakers may not (and should not) remain satisfied with purely voluntary systems, for two reasons. First, they may be normatively unsustainable. The standard, consent-based model of data privacy fits uneasily in the infectious-disease context. As Professor Jane Bambauer and others explain, "[I]t doesn't make sense, given the particular characteristics of this virus, to treat each individual's privacy choices as a matter for individual control."[89] Because a person's decision not to participate in a tracking program might put others at risk, "[a]s with lockdowns, the decision must be made at a collective level. A user choice conception of privacy must give way to other societal interests."[90] We can see the limits of a consent-based model in the debate over compulsory vaccination of schoolchildren.[91] Especially if the COVID-19 outbreak remains severe and digital disease surveillance proves effective, those individuals who refuse to participate in digital disease surveillance may increasingly be viewed akin to those parents that refuse to vaccinate their children, and thus spur legislation requiring participation.[92]

Second, evidence from other countries suggests that digital-disease-surveillance mandates are necessary for broad societal participation. In

87. *See* Public Health Emergency Privacy Act, S. 3749, 116th Cong. § 3(d) (2020) (making it unlawful for an organization to use emergency health data unless the individual "has given affirmative express consent"); *see also* COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong. § 3(a) (2020) (requiring "affirmative express consent" to use data).

88. S. 3749; S. 3663.

89. Bambauer et al., *supra* note 14.

90. *Id.*

91. Erwin Chemerinsky & Michele Goodwin, *Compulsory Vaccination Laws Are Constitutional*, 110 NW. U. L. REV. 589, 593–94 (2016).

92. *Cf. id.* at 603 (showing how parents' refusal to vaccinate their children requires compulsory vaccination legislation).

countries like Singapore[93] and Australia,[94] where participation in tracking apps is voluntary, participation levels have remained low,[95] thus rendering the programs ineffective.[96] There is no reason to think that voluntary programs will fare any better in the United States, especially given the extreme partisanship over the government's coronavirus response.[97] And there is no guarantee that private companies that surveillance regimes will act to maximize public health.[98]

---

93. Liza Lin & Chong Koh Ping, *Singapore Built a Coronavirus App, but It Hasn't Worked so Far*, WALL ST. J. (Apr. 22, 2020, 5:34 AM), https://www.wsj.com/articles/singapore-built-a-coronavirus-app-but-it-hasnt-worked-so-far-11587547805.

94. *See* Josh Taylor, *How Did the Covidsafe App Go from Being Vital to Almost Irrelevant?*, GUARDIAN (May 23, 2020, 4:00 PM), https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant (finding that Australia's Covidsafe app has been barely used since its launch).

95. *See id.* (reporting that only one person had used Australia's Covidsafe app a month after the launch); Lin & Ping, *supra* note 93 (showing that Singapore is far from reaching the minimum levels of resident participation that are needed for its contact tracing app to be effective).

96. The effectiveness of a contact tracing app is proportional to the square of the fraction of the population that uses it. Ferretti et al., *supra* note 60, at 5. It is uncertain precisely how adoption levels affect apps' effectiveness, although higher levels are more effective than lower levels. *See* Patrick Howell O'Neill, *No, Coronavirus Apps Don't Need 60% Adoption to Be Effective*, MIT TECH. REV. (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download [https://perma.cc/XT6H-EU96] (noting that even with low levels of coronavirus app adoption, simulations show benefits of using such apps).

97. *See* Shana Kushner Gadarian et al., *Partisanship, Health Behavior, and Policy Attitudes in the Early Stages of the COVID-19 Pandemic*, 16 PLOS ONE 1–2 (2021), (highlighting the "politicization of the public health response to COVID-19" in the United States and showing consistent partisan differences in behavior and responses to the pandemic); Amanda Graham et al., *Faith in Trump, Moral Foundations, and Social Distancing Defiance During the Coronavirus Pandemic*, 6 SOCIUS 1, 12 (2020) (showing that not only partisanship but faith in former President Trump is a "powerful predictor[] of intentions to defy social distancing directives").

98. *See* Reed Albergotti & Drew Harwell, *Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless*, WASH. POST (May 15, 2020, 3:22 PM), https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus (showing Google and Apple's contact tracing app prioritizes privacy over efficiency and does not share essential information with health officials or identify where a person may have been exposed); Stewart Baker, *The Problem with Google and Apple's COVID-19-Tracking Plan*, LAWFARE (Apr. 14, 2020, 12:14 PM), https://www.lawfareblog.com/problem-google-and-apples-covid-19-tracking-plan [https://perma.cc/JFT7-4LV5] (discussing the limitations of tracking apps developed by Google and Apple, which prioritize privacy over effectiveness); *see also* Julie E.

By contrast, many of the countries that did the best job dealing with the pandemic—primarily East Asian countries like South Korea, Taiwan, and China—have all used aggressive, mandatory digital disease surveillance.[99] While China's authoritarian political system makes it an inappropriate model for the American experience,[100] South Korea[101] and Taiwan[102] are both advanced liberal democracies and present a plausible model for the United States.

This is not to say that there is no room for voluntary programs. Governments could use behavioral nudges[103]—for example, requiring that digital-surveillance apps automatically be installed and activated on smartphones but allow users to manually disable them. They could incentivize participation, either by providing financial[104] or other incentives,[105] or by taxing or fining those who refuse to participate. But

---

Cohen, Woodrow Hartzog & Laura Moy, *The Dangers of Tech-Driven Solutions to COVID-19*, BROOKINGS (June 17, 2020), https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19 [https://perma.cc/6R5C-G7D2] ("Enshrining platforms and technology-driven 'solutions' at the center of our pandemic response cedes authority to define the values at stake and deepens preexisting patterns of inequality in society.").

99. Lewis, *supra* note 57.

100. *See* Lydia Khalil, *Digital Authoritarianism, China and COVID*, LOWY INST. (Nov. 2, 2020), https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid [https://perma.cc/3D9G-CQBM] (discussing China's digital authoritarian model).

101. *See, e.g.*, Kim, *supra* note 36 (showing the varied tools that South Korea has used to effectively contact trace and limit the coronavirus outbreak, including emergency texts, compulsory GPS-tracking apps, and government reports on confirmed cases, all of which may provide lessons for the United States).

102. *See, e.g.*, C. Jason Wang et al., *Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing*, 323 JAMA 1341, 1341 (2020) (discussing Taiwan's proactive response to the pandemic focusing on "[b]order [c]ontrol, [c]ase [i]dentification, and [c]ontainment").

103. *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6–8 (2008) (discussing how setting particular default options when choices can be made nudges people to a particular choice and can be powerful when combined with incentives).

104. *See* Jemima A. Frimpong & Stéphane Helleringer, *Financial Incentives for Downloading COVID-19 Digital Contact Tracing Apps*, CTR. FOR OPEN SCI. 3 (Working Paper, 2020), https://osf.io/download/5ed486adc7568603ce2d2e17 (assessing the potential of "providing financial incentives to potential users" and how it might increase the adoption of contact tracing apps).

105. One example is Harvard University's handling of a mumps outbreak in 2016. The university developed an early-diagnosis app which it encouraged students to use:

the more severe an epidemic becomes, the more policymakers will look to some degree of mandatory participation, thus raising the legal and policy issues that the rest of this Article addresses.

II. DIGITAL DISEASE SURVEILLANCE AND THE FOURTH AMENDMENT

This section examines the constitutionality of digital disease surveillance programs under the Fourth Amendment.[106] It argues that most digital disease surveillance programs would be subject to the Fourth Amendment but that they would generally pass constitutional muster.

A. When Does the Fourth Amendment Apply?

Before addressing the merits of a Fourth Amendment claim, two threshold questions must be addressed: is the surveillance attributable to the government and, if so, is it the kind of "search" that the Fourth

---

"We named the app House Call, because if you sign up and report symptoms, we'll come to you. We can bring you a testing kit along with honey and tea. Then, through the app, we can trace students' contacts. We may not be able to stop every spark of infection from lighting, but we can catch it before it becomes a fire." *See* Emily Bazelon, *What Will College Be like in the Fall*, N.Y. TIMES MAG. (June 25, 2020), https://www.nytimes.com/2020/06/03/magazine/covid-college-fall.html (quoting Harvard University professor, Dr. Pardis Sabeti). The line between incentives and punishments is a fuzzy one. For example, a contact tracing proposal released by the center-left think tank Center for American Progress would make individuals' eligibility to receive testing for coronavirus contingent upon their using a contact-tracing app. Zeke Emanuel et al., *A National and State Plan to End the Coronavirus Crisis*, CTR. FOR AM. PROGRESS (Apr. 3, 2020, 7:00 AM), https://www.americanprogress.org/issues/healthcare/news/2020/04/03/482613/national-state-plan-end-coronavirus-crisis [https://perma.cc/PBQ8-BC9G].

106. This is not to say that other individual-rights provisions of the Constitution are irrelevant to disease surveillance. *See* GOSTIN & WILEY, *supra* note 11, at 115–17 (examining public health powers in relation to the First, Second, Fourth, and Fifth Amendments). For example, the First Amendment may limit the extent to which digital disease surveillance programs can track people's movements and personal interactions, given the potential chilling effect of such surveillance on First Amendment associational rights. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154, 155, 157, 158 (2007). The Fifth Amendment's ban on compulsory self-incrimination may limit the extent to which information from mandatory contact tracing or location apps can be used in a criminal case. And the Fourteenth Amendment's guarantee of equal protection may prohibit states from imposing digital disease surveillance in a discriminatory manner. Nevertheless, the application of Fourth Amendment doctrine and principles is most straightforward and so is the focus of this Article.

Amendment regulates? The answer to both of these questions will generally be yes.

1. The state-action requirement

The Fourth Amendment only regulates action taken by the government or its agents. Its protections do not apply to activity taken solely by private entities,[107] including when private entities independently and voluntarily share data (including electronic data[108]) with the government.[109] Thus, if a private company were to create a disease surveillance program and then share that information with public health authorities (as the Apple-Google plan appears to do), the Fourth Amendment is not triggered.[110] However, if the government requires companies to turn over data they have collected for their own purposes, forces them to engage in surveillance in the first place, or simply engages in a "joint endeavor" with a private party,[111] then the state-action requirement is met, and the Fourth Amendment applies in full.[112] Even government action that merely

107. Burdeau v. McDowell, 256 U.S. 465, 467 (1921).

108. *See* United States v. Reddick, 900 F.3d 636, 637–38 (5th Cir. 2018) (holding that no Fourth Amendment search existed where private cloud hosting service "automatically scan[ned] the hash values of user-uploaded files and compare[d] them against the hash values of known images of child pornography" and then sent positive matches to the government).

109. Under the "private search" doctrine, the government may replicate the search of an object first conducted by a private entity and supplied to the government by that entity. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("[W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."); United States v. Lichtenberger, 786 F.3d 478, 481, 483–84 (6th Cir. 2015) (holding that the *Jacobsen* standard for private searches applied when an individual searched her boyfriend's laptop and later showed a police officer some of what she found on the laptop, because she was acting as a private citizen at the time of the search).

110. Though statutes may nevertheless limit the extent to which private entities can share data with the government. *See, e.g.*, 18 U.S.C. § 2702 (preventing providers of "remote computing service[s] or electronic communication service[s]" from sharing subscriber information with any governmental entity).

111. Corngold v. United States, 367 F.2d 1, 6 (9th Cir. 1966).

112. A good real-world example of the complexity of Fourth Amendment state-action analysis is in the complex legal regime that governs how internet platform and services share information with the government about child exploitation material they detect on their services. *See, e.g.*, United States v. Ackerman, 831 F.3d 1292, 1294–95 (10th Cir. 2016) (discussing whether AOL screening for child pornography of an email

facilitates, rather than directly requires, private searches can establish state-action.[113]

As with most legal distinctions, the line between purely private searches and those that fall under the Fourth Amendment's scope is a fuzzy one, and the applicable doctrine is complex.[114] To simplify the analysis, and because purely voluntary surveillance programs will likely be insufficient to meet the current public health challenges,[115] this Article will assume that state-action is satisfied with respect to the digital disease surveillance programs discussed below.

2. The search requirement

The second threshold question is whether the surveillance activity is a "search." Surveillance is a search and thus triggers the Fourth Amendment if it infringes on a reasonable expectation of privacy (the *Katz*[116] test) or if it involves a government trespass on property (the

---

account which forwards the information to the National Center for Missing and Exploited Children—which confirms the presence of child pornography and alerts law enforcement—requires Fourth Amendment protection), *aff'd*, 804 F. App'x 900 (10th Cir. 2020); Jeff Kosseff, *Online Service Providers and the Fight Against Child Exploitation: The Fourth Amendment Agency Dilemma*, LAWFARE (Jan. 18, 2021, 9:42 AM), https://www.lawfareblog.com/online-service-providers-and-fight-against-child-exploitation-fourth-amendment-agency-dilemma [https://perma.cc/BVS9-H7NR] (arguing that private companies might be treated as government agencies subject to the Fourth Amendment if they work closely with law enforcement during an investigation into child exploitation).

113. *See, e.g.*, Skinner v. Ry. Lab. Execs. Ass'n, 489 U.S. 602, 614–16 (1989) (finding that the "Government's encouragement, endorsement, and participation" in a search by a private company is sufficient to implicate the Fourth Amendment).

114. *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 1.8 (6th ed. 2020) ("[T]he issue of precisely what it takes to put a search outside the 'private' category is frequently litigated in a wide variety of settings.").

115. *See supra* notes 84–105 and accompanying text.

116. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (creating a two-part test by which a search has occurred under the Fourth Amendment if an individual's subjective expectation of privacy has been violated and the expectation is reasonable). The question of what government conduct infringes upon a reasonable expectation of privacy is a notoriously complicated one. As I have previously noted, "Anyone who has struggled to learn, teach, or apply *Katz*'s reasonable-expectation-of-privacy standard to the broad variety of real-world policing scenarios will appreciate why Fourth Amendment doctrine is so frequently characterized as 'a mess,' 'an embarrassment,' and 'a mass of contradictions.'" Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J. F. 943, 959 n.82 (2019) (quoting Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth*

Jones[117] test). Different forms of disease surveillance could trigger the Fourth Amendment under one or both of these tests. For example, any government surveillance program that requires individuals to download an app on their phones might constitute a Fourth Amendment search under the *Jones* trespass test, since it would interfere with individuals' property interests—that is, to control what is on their devices.[118] By contrast, were the government to track people's movement by directly surveilling cellphones, that might violate a person's reasonable expectation of privacy under *Katz*.[119]

Things become more complex if the government was to compel third-parties—cellphone companies, internet platforms, medical-device makers, or health-care providers—to turn over data. A long-established (and much criticized[120]) carve out to the *Katz* reasonable-expectation-of-privacy test is the "third-party doctrine": people cannot claim a reasonable expectation of privacy in information they have voluntarily handed over to a third-party and that the government subsequently acquires.[121]

Amendment, 125 HARV. L. REV. 476, 479 (2011)). Professor Orin Kerr argues that, at least at a high level of generality, the Supreme Court applies the *Katz* test (and the Fourth Amendment in general) so as to maintain a status quo of police power in the face of changing technology. Kerr, *supra* note 116, at 480. But on a case-by-case basis the development of the *Katz* test is still difficult to predict.

117. *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that it is a sufficient condition for a Fourth Amendment search that "[t]he Government physically occupied private property for the purpose of obtaining information").

118. *Id.* at 414 (Sotomayor, J., concurring) (noting the "longstanding protection for privacy expectations inherent in items of property that people possess or control").

119. *See, e.g.*, Jones v. United States, 168 A.3d 703, 713 (D.C. Cir. 2017) (holding that "the use of a cell-site simulator to locate [the defendant's] phone invaded a reasonable expectation of privacy and was thus a search"); *see also supra* note 119 (describing the *Katz* reasonable expectation test).

120. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) (describing common criticisms of the third-party doctrine).

121. *See* Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (holding that the plaintiff had no expectation of privacy with respect to telephone numbers he dialed because the information was voluntarily given to a third party, and he "assumed the risk that the company would reveal to police the numbers he dialed"); United States v. Miller, 425 U.S. 435, 440, 443 (1976) (holding that no Fourth Amendment protection is required when the respondent's bank turned over bank records in response to a subpoena).

But the third-party doctrine may not apply to digital disease surveillance. In *Carpenter v. United States*,[122] the Supreme Court held that the third-party doctrine did not apply to a week's worth of cellphone location data that the government had acquired from a mobile provider.[123] The Court did so on the grounds that the information—even if it had been shared with a third-party—"provide[d] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[124]

Unfortunately, the Court did not provide much guidance on how to apply *Carpenter*'s reasoning to different fact patterns: smaller amounts of more precise location data, larger amounts of less precise location data, non-location data (for example, health data) that nevertheless reveals intimate information about an individual, and so on. Lower courts have been left to grapple with the question of whether data that would normally be excluded from the Fourth Amendment's scope under the third-party doctrine is nevertheless protected because it is particularly sensitive and revealing.[125] Given its sensitivity, health information plausibly falls under this category.[126]

---

122. 138 S. Ct. 2206 (2018).

123. *Id.* at 2216–17.

124. *Id.* at 2217 (citing Jones v. United States, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

125. *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 361–66 (2019) (highlighting how the broad nature of the *Carpenter* case allows criminal defendants to test the boundaries of the rule). For arguments that *Carpenter*'s cabining of the third-party doctrine should be read broadly, see Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 6–7, 12 (2020); Rozenshtein, *supra* note 115, at 952–53.

126. Judicial treatment of this issue has been limited but evidences a recognition that health information is sensitive. The Supreme Court has recognized that prescription-drug information implicates privacy interests, Whalen v. Roe, 429 U.S. 589, 598–600 (1977), and that the "reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001). The sensitivity of medical information is also reflected in the extensive federal and state legislation and regulation on health privacy. *E.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, §§ 263–64, 110 Stat. 1936, 2031, 2033–34 (federal); JOY PRITTS ET AL., THE STATE OF HEALTH PRIVACY: A SURVEY OF STATE HEALTH PRIVACY STATUTES (2d ed. 2002) (state).

B. What Does the Fourth Amendment Require?

Assuming the Fourth Amendment does apply to government surveillance, the Fourth Amendment requires that the activity be "reasonable."[127] In most cases, reasonableness requires that the government have probable cause and get a magistrate's authorization—a warrant—before conducting the search.[128] In some cases this may be feasible. For example, if the government gets a reliable tip that an infected individual has violated a quarantine order, that might be enough to establish probable cause that a crime has been committed (the quarantine violation) and thus justify a warrant for location data to confirm this fact.

But for many public health purposes, strict adherence to a warrant regime may not be required. One doctrinal option is the "exigent circumstances" exception, which permits the government to dispense with warrants where the circumstances render them unfeasible.[129] For example, police do not need a warrant to arrest a fleeing suspect or to prevent the destruction of evidence.[130] Nor is a warrant required when police are acting to render "emergency aid" to someone.[131] But courts tend to construe these exceptions narrowly, and, most importantly, they still require police to have probable cause that the underlying activity is taking place.[132] These exceptions to the warrant requirement thus are unlikely to be sufficient for disease surveillance, which requires gathering ongoing data on a wide population (rather than individual by individual), of which few if any may have clear symptoms.[133]

---

127. U.S. CONST. amend. IV.

128. *See id.* (requiring that "no [w]arrants" be "issue[d], but upon probable cause"); Coolidge v. New Hampshire, 403 U.S. 443, 449 (1971) (invalidating a search warrant that was not issued by a "neutral and detached magistrate").

129. Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–99 (1967).

130. *See, e.g.*, *id.* (finding exigent circumstances in the context of arresting a fleeing suspected felon); Kentucky v. King, 563 U.S. 452, 455 (2011) (finding that "exigent circumstances" encompass preventing the destruction of evidence).

131. *King*, 563 U.S. at 460.

132. *See, e.g.*, *Hayden*, 387 U.S. at 309–10 (finding police had the requisite probable cause to lawfully enter and search the home of a suspected felon who fled inside).

133. This is not only because many tracked individuals will not be infected, but also because, according to the CDC's best current estimates, forty percent of infected individuals will not exhibit any symptoms at all. *COVID-19 Pandemic Planning Scenarios*, CDC (Sept. 10, 2020), https://www.cdc.gov/coronavirus/2019-ncov/hcp/planning-scenarios.html [https://perma.cc/QKP8-HKKN]. The high potential for both false positives and false negatives makes probable cause very difficult to establish.

For this reason, any disease surveillance program is likely to be principally evaluated under the Fourth Amendment's "special needs" (also called the "administrative search") doctrine.[134] Here, courts sometimes permit warrantless surveillance with less than probable cause if getting a warrant would be impracticable, the search is aimed at something other than a traditional law enforcement purpose, and the search is, all things considered, reasonable.[135]

As Professor Eve Brensike Primus has explained, the modern special-needs doctrine is the descendent of two earlier lines of cases.[136] The first relaxed the requirement of individualized suspicion for "dragnet search[es] . . . in which the government searches or seizes every person, place, or thing in a specific location or involved in a specific activity based only on a showing of a generalized government interest."[137] These searches nevertheless had to limit executive discretion, either through some sort of judicial authorization (albeit short of a warrant), or by a comprehensive statutory or administrative structure.[138]

The second line of cases permitted searches of "special subpopulation[s]"—groups of individuals with "reduced expectations of privacy"—without probable cause.[139] Unlike dragnet searches, officials could exercise broad discretion in searching special subpopulations, but they also had to establish individualized suspicion (even if less than probable cause) before searching.[140]

Had these two lines of cases stayed separate, they would have provided a useful doctrinal framework for analyzing digital disease surveillance. Contact tracing apps could be analyzed as dragnets (since they would be applied across groups and by their very nature could not support individualized suspicion), while tracking to enforce quarantine and isolation would be analyzed as searches of special subpopulations, namely those for which there is individualized suspicion to believe they are infected or are under high risk.

---

134. City of Los Angeles v. Patel, 576 U.S. 409, 420 (2015).

135. *Id.*

136. *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 261–62 (2011).

137. *Id.* at 263.

138. *Id.* at 267.

139. *Id.* at 260.

140. *Id.* at 271–72.

Unfortunately, as Primus notes, the doctrinal distinction between dragnets and special subpopulations searches collapsed throughout the 1970s and 1980s.[141] The Supreme Court began to analyze both types of searches under what it called the "special needs" test,[142] which jettisoned both the requirement of minimizing discretion (for dragnets) and individualized suspicion (for searches of special subpopulations) in favor of open-ended "reasonableness balancing."[143]

The result has been a doctrine that not only undermines key Fourth Amendment values, but is hopelessly incoherent and unsettled, full of seemingly arbitrary distinctions that appear to reflect little more than the gut instincts of shifting majorities on the Supreme Court. For example, vehicle checkpoints are permissible when aimed at drunk driving[144] but not at intercepting drugs.[145] Discretionary stops of vehicles to check licenses are not permitted,[146] but similar stops of ships are.[147] Searches of students generally require some degree of individualized suspicion,[148] but student athletes[149] or anyone engaging in extracurricular activities[150] can be subjected to blanket mandatory drug testing. The list of random-seeming fact patterns goes on.[151]

It remains difficult to predict when the courts will authorize nontraditional surveillance under the special-needs doctrine. As Professor Christopher Slobogin notes, however, the only factor that even approximates a clear doctrinal requirement is that the government demonstrate a need for surveillance that goes beyond the

---

141. *Id.* at 276–77, 302.

142. Justice Blackmun first articulated this test in *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment), and then the Supreme Court adopted it in *New York v. Burger*, 482 U.S. 691, 702 (1987).

143. Primus, *supra* note 136, at 277; *see also* United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983) (describing the focus in a Fourth Amendment administrative search as one of "reasonableness" in balancing intrusion on the individual with promotion of a legitimate governmental interest).

144. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990).

145. City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000).

146. Delaware v. Prouse, 440 U.S. 648, 663 (1979).

147. *Villamonte-Marquez*, 462 U.S. at 593.

148. New Jersey v. T.L.O., 469 U.S. 325, 341–42 (1985).

149. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 648, 664–65 (1995).

150. Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822, 825 (2002).

151. *See generally* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 3.9 (4th ed. 2020) (providing additional examples of Fourth Amendment special-needs searches).

purposes of ordinary law enforcement.[152] Once this factor is met, courts engage in a fairly open-ended balancing inquiry in which the government interest is accorded great weight.[153]

C. Most Digital Disease Surveillance Satisfies the Fourth Amendment

Under the current special-needs doctrine, digital disease surveillance would generally satisfy the Fourth Amendment.[154] This is because the Supreme Court's "dragnet jurisprudence leaves considerable room for play."[155] The main complication would be if law enforcement had a primary and substantial role in such surveillance, and even then, the surveillance might be permissible.[156]

With respect to contact tracing, if the government requires people to download contact tracing apps on their phones, that might trigger the Fourth Amendment under the *Jones* trespass test.[157] If instead the government were to collect large amounts of location data from companies, that would likely trigger the Fourth Amendment under the *Katz* reasonable-expectation-of-privacy test, especially in light of *Carpenter*.[158]

Thus, the constitutionality of contact tracing would hinge on the special-needs analysis. The key factor—that the surveillance not be for a traditional law-enforcement purpose—would likely be easy to satisfy. And given the severity of the coronavirus pandemic, both in terms of public health and economic damage, courts would likely permit digital contact tracing programs as long as the government can demonstrate some level of effectiveness.

---

152. Christopher Slobogin, *Government Dragnets*, 73 L. & CONTEMP. PROBS. 107, 126–27 (2010) [hereinafter Slobogin, *Government Dragnets*].

153. *Id.* at 111, 127–28.

154. Others have come to similar conclusions. *See, e.g.*, Ram & Gray, *supra* note 9, at 9 ("The epidemiological surveillance programs discussed in recent months . . . are likely to fall under the special needs doctrine because their purpose is to address public health challenges rather than to effect the goals of traditional law enforcement."). For an earlier Fourth Amendment analysis of disease surveillance, see Richards, *supra* note 9, at 34–43.

155. Slobogin, *Government Dragnets*, *supra* note 152, at 127. By "dragnet," Slobogin means "searches and seizures of groups" that "attempt to cull out bad actors through ensnaring a much larger number of individuals who are innocent of any wrongdoing." *Id.* at 108.

156. *See infra* notes 164–69.

157. *See supra* notes 117–18 and accompanying text.

158. *See supra* notes 119–24 and accompanying text.

Tracking to enforce isolation and quarantine poses a more complicated legal question.[159] As above, a threshold question is how the government collected the information at issue. If the government required infected individuals to download a location-broadcasting app on their phones—or, in an extreme case, to wear a physical device, like a GPS bracelet—that would almost certainly trigger the Fourth Amendment under *Jones*.[160] If the government instead tracked the quarantined person's phone directly (for example, through IMSI catchers)[161] or indirectly (by compelling the disclosure of location data from the cellphone provider), whether the activity was a search would likely turn on how much information the government acquired.[162]

---

159. And a separate one from the legality of the quarantine/isolation itself, which raises difficult due process issues. *See generally* Wendy E. Parmet, *Quarantining the Law of Quarantine: Why Quarantine Law Does Not Reflect Contemporary Constitutional Law*, 9 WAKE FOREST J.L. & POL'Y 1, 21–29 (2018) (explaining the lack of clarity about the constitutional constraints on quarantine).

160. *See supra* notes 117–18 and accompanying text.

161. *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185, 191–92 (2014) (explaining that International Mobile Subscriber Identifier (ISMI) catchers deceive nearby cell phones into believing the device is a cell tower, thereby allowing users, like law enforcement, to intercept audio and data content).

162. If the surveillance only disclosed when individuals left the quarantine zone, that would substantially strengthen the argument for constitutionality, especially absent a physical intrusion into the quarantined person's phone. *Cf.* Grady v. North Carolina, 575 U.S. 306, 308–09 (2015) (per curiam) (holding that, under *Jones*, compulsory electronic monitoring of a sex offender by means of an ankle bracelet was a Fourth Amendment search). Indeed, the program might not even count as a Fourth Amendment search at all. Under the "binary search" doctrine, government action that only discloses whether or not some contraband or other illicit substance is present is not a search, on the theory that no one has a reasonable expectation of privacy in breaking the law. *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1348–51 (2002) (describing a "binary search" as one in which "the technology used is designed in such a way that the only result of the investigation is information about whether contraband or illegal activity is present"). The binary search doctrine has been most commonly applied in the context of drug-sniffing dogs, *United States v. Place*, 462 U.S. 696, 707 (1983), or drug field tests, *United States v. Jacobsen*, 466 U.S. 109, 123 (1984), but the same logic might apply here. Especially if leaving a quarantine zone would violate the law, a system that notified the government only when someone left the zone might avoid Fourth Amendment scrutiny altogether. Of course, the binary search doctrine is in tension with the special-needs doctrine's emphasis on data not being used for law enforcement purposes. How these two doctrines can be harmonized—other than by

If the surveillance was a search, whether it was nevertheless reasonable in the absence of a warrant would turn on the intrusiveness of the search relative to its importance in enforcing quarantine. Because enforcing a quarantine does not require constant surveillance of people while they are in the quarantine zone but rather only when they leave it, broad and constant surveillance would likely not pass constitutional muster, especially if the surveillance disclosed information about people's activities inside their homes.[163] Although the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment,"[164] the health and safety benefits of the search must still outweigh its privacy costs.

Another important factor would be whether the data was available for criminal prosecutions. Unlike contact tracing, which does not seek to deter conduct, surveillance for quarantine and isolation does. If quarantine and isolation requirements were backed up with criminal penalties, surveillance could potentially run afoul of the requirement that the "relevant primary purpose" of a special-needs program not be a traditional law enforcement purpose.[165]

An illustrative case is *Ferguson v. City of Charleston*,[166] in which the Court struck down a program by which pregnant women were subject to nonconsensual drug tests, the results of which were shared with the police, leading to prosecutions for child abuse (of the fetus).[167] Although the program in *Ferguson* undoubtedly had a public health dimension, "the central and indispensable feature of the policy from its inception was the use of law enforcement to coerce the patients into

---

simply excluding binary searches from the Fourth Amendment's scope—is an open question.

163. *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding that the Fourth Amendment did not apply when the government placed a location-monitoring beeper in a package that was transported to the defendant's home), *with* United States v. Karo, 468 U.S. 705, 714 (1984) (holding that the Fourth Amendment applied where the government monitored a location-tracking beeper while it was located in the defendant's home), *and* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the Fourth Amendment applied where police used thermal imaging to detect heat signatures from inside a house).

164. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995).

165. Ferguson v. City of Charleston, 532 U.S. 67, 81 (2001).

166. 532 U.S. 67 (2001).

167. *Id.* at 84–86.

substance abuse treatment"[168] and was thus "ultimately indistinguishable from the general interest in crime control."[169] *Ferguson* is particularly relevant because it too involved a kind of surveillance for disease, in that case substance abuse disorder, suggesting that digital disease surveillance for pandemic detection and control would still be subject to the "relevant primary purpose" test.[170]

Then again, *Ferguson* should not be pushed too far. The Supreme Court has repeatedly permitted secondary prosecutions under special-needs programs.[171] Whether a quarantine/isolation program that relies on warrantless surveillance could be criminally enforced is an uncertain question. Presumably, a program that leads to frequent criminal enforcement would be more vulnerable to Fourth Amendment challenges than one in which the criminal law is used as a last resort (e.g., after several warnings to the individual) and only against the most egregious violators.

* * *

As the above analysis shows, Fourth Amendment doctrine imposes relatively few constraints on digital disease surveillance (though given the confused state of much of the law, any predictions should be taken with a grain of salt). This naturally raises two further questions, which are the focus of the remainder of this Article.

The first question is: are there additional safeguards that, while not required by current Fourth Amendment doctrine, would further Fourth Amendment values and are nevertheless compatible with aggressive digital disease surveillance? In other words, can digital disease surveillance be more *efficient* (with respect to privacy and civil liberties) than the Fourth Amendment currently requires it to be? As I argue in Part III, the answer is yes.[172]

---

168. *Id.* at 80.

169. *Id.* at 81 (quoting City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000)).

170. *Id.* at 81–83.

171. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 347–48 (1985) (reversing suppression of evidence found during search of student's purse); Griffin v. Wisconsin, 483 U.S. 868, 872–73 (1987) (permitting warrantless, supervisory search of probationer's home pursuant to state regulation that was deemed a reasonable "special need").

172. Part III thus provides additional support (although it is not the main focus of the Article) for criticisms that the Fourth Amendment insufficiently protects Fourth Amendment values, at least when it comes to programmatic surveillance. *See infra* Part III; *see also* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE,

The second question is: given the inadequacy of current Fourth Amendment doctrine to ensure the efficiency of digital disease surveillance, how should courts, the main interpreters of the Fourth Amendment, respond? In Part IV, I outline a set of principles that courts should follow in updating the Fourth Amendment to take into account the safeguards discussed in Part III. I also argue that this updating should apply beyond the disease surveillance context, to include other forms of programmatic digital surveillance.

III. EFFICIENT DIGITAL DISEASE SURVEILLANCE

Although courts decide most special-needs cases solely based on whether the government has a legitimate need for surveillance that goes beyond traditional law enforcement purposes, the doctrine is littered with additional factors that courts purport to consider, including the proportionality of the government action, an inquiry that balances the intrusiveness of the search against the expected government benefits of that search and also asks whether the government could achieve its objective using less intrusive means; the presence or absence of legislative authorization and strict administrative guidelines; and the presence or absence of judicial supervision, whether ex ante or ex post.[173] This section explores what it would look like to take these and other relevant factors seriously. It outlines a set of safeguards that could enhance privacy and civil liberties while generally preserving the effectiveness of digital disease surveillance programs.

A useful way of conceptualizing this set of safeguards is to ask what features of a digital disease surveillance program could be used to increase its *efficiency*, as that term is understood in economic analysis. In the context of disease surveillance, for a given amount of public

---

RACE, AND THE FUTURE OF LAW ENFORCEMENT 140–42 (2017) (discussing distortions of big data policing, which skew the reasonable-suspicion decision to stop individuals, and noting that predictive policing technologies may "mark out areas of lesser Fourth Amendment protection"); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1053–56 (2016) (describing three types of problems programmatic surveillance poses for a "transactional Fourth Amendment framework"); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 59–63 (2014) (arguing police access to big data due to enhanced surveillance capacities should alter Fourth Amendment protections).

173. Slobogin, *Government Dragnets*, *supra* note 152, at 126–27.

health (H) there will be some maximum amount of privacy (P) that we can enjoy (because of the necessary amount of surveillance and information collection that is required to prevent further spread of disease). Thus, if we want to have a level of privacy P^* greater than P, the corresponding level of public health, H^*, will be lower than H. The set of points that maximize privacy for a given level of health (and vice-versa) is the *production-possibility frontier* for health and privacy.[174] Points beyond the frontier are unavailable to society given its current resources (which includes its level of technological advancement and organizational capacity). Points on the frontier are "efficient" (or more precisely "Pareto efficient"). And points within the frontier are "inefficient," since it is possible to move from that point to another one without sacrificing either safety or privacy.

This model is useful because it separates two questions that are often conflated: whether it is desirable to be on the frontier versus where on the frontier it is desirable to be. The first question is an easy one: it is always better to be on the frontier than to be within it (remembering that being beyond it is impossible), because it is better to be efficient than inefficient. The second question is much harder: the optimal tradeoff between health and privacy (as between any two goods) depends on a complex combination of individual preferences, social utility functions, distributional considerations, and prior normative commitments. But the difficulty in making progress on the second question should not blind us to the possibility of making progress on the first.[175] The safeguards suggested in this Part can all be viewed as ways of answering the first question, specifically by making digital disease surveillance programs more rights protective while still effective (either by imposing no or minimal public health costs), and

---

174. I take this model from Eric A. Posner and Adrian Vermeule, who used it to discuss the case of national security versus liberty. ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY, AND THE COURTS 26–27 (2007). For its application to surveillance policy, see Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 163–71 (2018). For a similar approach, see RIC SIMMONS, SMART SURVEILLANCE: HOW TO INTERPRET THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 8–10 (2019), which I review in *Cost-Benefit Analysis and the Digital Fourth Amendment*, 40 CRIM. JUST. ETHICS 75 (2021) (reviewing SIMMONS, *supra*).

175. Although we cannot theorize our way towards a right answer for what is the optimal point on the frontier, we can still draw second-order conclusions as to who should decide what point on the frontier is chosen. *See infra* notes 281–83 and accompanying text.

thus should be attractive whether one's primary concerns are with public health or civil liberties (or any combination of the two).

I divide the safeguards into three categories. The first, *outcomes*, looks to the effects the program has: does it work, and for whom? The second, *institutional design*, considers the inner workings of digital disease surveillance. The third, *democratic authorization*, ensures that surveillance programs satisfy core democratic principles.

A. Outcomes

At a minimum, public policy should work (achieve its goal) and do so fairly, without imposing disproportionate costs on any small groups, especially if those groups are already disadvantaged. But often even these basic requirements of substantive rationality are not met. To satisfy these requirements in the case of digital disease surveillance, policymakers at the front end, and those that review their work at the back end (courts and the public), will need a structured framework to evaluate both *effectiveness* and *fairness*,[176] which this Part addresses in turn.

1. Effectiveness

A key change in the regulatory state over the past two decades has been the widespread adoption of cost-benefit analysis: the attempt to, as rigorously as possible (and whether quantitively or qualitatively), measure the net effects of a government program on overall societal welfare.[177] Despite its broad adoption, one area of public policy has remained stubbornly free from its scope: surveillance.

Why this unfortunate absence? For starters, the main agents of surveillance—from state and local police departments up through federal law enforcement, national security, and foreign-intelligence agencies—are by law or practice excluded from the foundational

176. Or, in the language of economics, welfare and fairness. *See generally* Louis Kaplow & Steven Shavell, *Fairness Versus Welfare*, 114 HARV. L. REV. 961, 976–79 (2001) (exploring the use of welfare economics and notions of fairness to evaluate legal rules).

177. Cass Sunstein in particular has been this change's chief champion and chronicler. *See generally* CASS R. SUNSTEIN, THE COST-BENEFIT REVOLUTION 3–4 (2018) (an overview of the pervasive use of cost-benefit analysis in the modern regulatory state); CASS R. SUNSTEIN, THE COST-BENEFIT STATE: THE FUTURE OF REGULATORY PROTECTION 6–10 (2002) (an early influential argument for cost-benefit analysis).

administrative law principles (like, at the federal level, the Administrative Procedure Act) that would facilitate systematic review of effectiveness.[178] Second, because surveillance implicates core values on both sides—public safety on the one hand and core constitutional rights on the other hand—the discourse around it can easily degenerate into a "taboo trade-off,"[179] with each side standing on principle, trivializing the other's position, impervious to the messy reality of data and compromise.[180]

But it should not, in principle, be impossible to apply cost-benefit analysis to surveillance programs.[181] This is especially true for disease surveillance programs, for two reasons. First, epidemiology is a sophisticated quantitative discipline, and the key metrics for any disease surveillance program—the number infected, the rate of spread, the location of highest contagion—are routinely and continuously modelled and calculated.[182] Second, unlike surveillance for law enforcement or national security purposes, surveillance for disease prevention can and should be transparent,[183] with both the details of the surveillance methods and the resulting data (appropriately

178. The reasons for this absence are complicated. In the case of national security and foreign-intelligence surveillance, the Administrative Procedure Act explicitly excludes "a military or foreign affairs function of the United States." 5 U.S.C. § 553(a)(1). In the case of policing, whether at the federal or state levels, federal and state administrative procedure regimes either explicitly exempt law enforcement agencies or have been interpreted to do so by courts. *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1839 (2015) (arguing that all police practices should be legislatively authorized and adopted through a democratic process, and describing the administrative rulemaking process).

179. *See* Philip E. Tetlock, *Thinking the Unthinkable: Sacred Values and Taboo Cognitions*, 7 TRENDS IN COGNITIVE SCI. 320, 322 (2003) (defining a "taboo trade-off" as one which "pit[s] sacred values against secular ones").

180. *See* Rozenshtein, *supra* note 174, at 165 (noting the trade-off between public safety and constitutional requirements in surveillance).

181. *See* Cass R. Sunstein, *Beyond Cheneyism and Snowdenism*, 83 U. CHI. L. REV. 271, 284–87 (2016) (describing the challenges of a cost-benefit analysis for surveillance programs and proposing that break-even analysis may provide more tangible results).

182. *See generally* Hernán De Battista et al., *On Key Epidemiological Metrics during Infectious Disease Outbreaks*, ARXIV (Nov. 4, 2020), https://arxiv.org/abs/2011.02516 (describing how the foregoing metrics are used to calculate an infectious disease's effective reproduction ratio (R_e) and doubling time to determine the sufficiency of potential health interventions).

183. *See infra* Section III.B.6.

deidentified) widely available for analysis, both by the government and independent researchers.

Of course, not all the effects of digital disease surveillance will be quantifiable. Models are an imperfect representation of reality, data is incomplete, some of the foundational assumptions behind cost-benefit analysis are contestable (what is the proper way of measuring the value of a statistical life?[184]), and certain values may be difficult to reduce to dollar estimates. But even with these limitations, governments have the capacity to provide more rigorous justifications for digital disease surveillance programs than for other types of surveillance.

This increased quantifiability has constitutional implications as well. Scholars have long called for greater use of proportionality analysis in American constitutional law, including as applied to the Fourth Amendment, both to expand individual rights[185] and to better balance them against societal interests.[186] In particular, Slobogin has, over a series of works, provided a comprehensive framework for applying proportionality thinking to Fourth Amendment issues.[187] In the context of programs that lack individualized suspicion, Slobogin advocates for "generalized suspicion"[188] (or, in the more stringent case,

---

184. *See generally* John Bronsteen et al., *Well-Being Analysis vs. Cost-Benefit Analysis*, 62 DUKE L.J. 1603, 1657 (2013).

185. *See* Vicki C. Jackson, *Constitutional Law in an Age of Proportionality*, 124 YALE L.J. 3094, 3130–36 (2015) (suggesting that a greater reliance on proportionality would enhance the protection of individual rights under the Fourth Amendment relative to the "categorical approach" employed by the Supreme Court).

186. *See* Jamal Greene, *Foreword: Rights as Trumps?*, 132 HARV. L. REV. 28, 124–27 (2018) ("Proportionality jurisdictions tend to engage these weighty questions [of tradeoffs] directly rather than load them onto a definitional frame that cannot bear their weight.").

187. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21–47 (2007) [hereinafter SLOBOGIN, *Privacy at Risk*] (reconceptualizing the Fourth Amendment using proportionality to deem a search or seizure reasonable "if the strength of its justification is roughly proportionate to the level of intrusion"); *see also* Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 68–75 (1991) (advocating for proportionality in the level of certainty necessary to authorize police action relative to the level of its intrusiveness); Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1070–77 (1998) (proposing a refined framework of the proportionality principle articulated in *Terry*) [hereinafter Slobogin, *Let's Not Bury* Terry].

188. SLOBOGIN, *Privacy at Risk*, *supra* note 187, at 40.

"generalized probable cause"[189]). Professor Daphna Renan has a similar idea, which she calls "administrative efficacy review": before starting a surveillance program, the government would publish a "programmatic probable cause determination."[190] Professor Ric Simmons advocates for cost-benefit analysis as the core of "smart surveillance."[191]

A difficulty with applying proportionality to traditional surveillance programs is that law enforcement and national security are not domains that have traditionally been subject to quantitative analysis. Thus, when trying to apply proportionality analysis to traditional surveillance programs, courts have struggled to do so with any degree of rigor (a difficulty which no doubt explains part of why courts often resist proportionality as a method of Fourth Amendment analysis). But proportionality should be easier to apply where, as in the disease surveillance context, the costs and benefits are more readily quantifiable.

Ultimately there is no one right answer as to how much privacy is worth sacrificing to slow the spread of disease. Different people—and thus different polities—will choose to make different tradeoffs.[192] Nevertheless, a focus on effectiveness can help policymakers identify areas of broad agreement. First, it can highlight situations at the extremes, in which giving up small amounts of privacy can lead to massive gains in public health, and vice versa. Second, it illustrates policy options that impose what Professor Cass Sunstein has called "gratuitous costs": situations in which privacy or public health are *unnecessarily* sacrificed, and where a change to the policy can lead to a win-win improvement for both values.[193] As Professors Lawrence Gostin and Lindsay Wiley have argued, "[p]ublic health depends on the community's trust and cooperation, and failure to safeguard privacy discourages participation in programs such as screening, partner notification, and medical treatment."[194] Third, simply requiring policymakers to explicitly attend to costs and benefits can improve

189. Slobogin, *Government Dragnets*, *supra* note 152, at 139.

190. Renan, *supra* note172, at 1108, 1112.

191. SIMMONS, *supra* note 174; *see also* Rozenshtein, *supra* note 174 (reviewing SIMMONS, *supra* note 174).

192. The implications of this point for judicial review are addressed *infra* Section IV.A.

193. Sunstein, *supra* note 181, at 287–88. Gratuitous costs correspond to policy choices that lie within the Pareto frontier. *See supra* notes 174–77 and accompanying text.

194. GOSTIN & WILEY, *supra* note 11, at 307.

their decision-making, limiting sloppy thinking and promoting more intelligent policy.[195]

2. Fairness

Most of us do not only care about effectiveness. We also value fairness, which requires that costs and benefits be distributed proportionally across society. Poorly designed digital disease surveillance programs can fail this requirement in two ways.

First, certain groups may not get the full benefits of digital disease surveillance. For example, while over 90% of Americans with an annual household income greater than $50,000 own smartphones (and thus could run contact tracing apps), that number drops to 71% for those with a household income below $30,000, 71% for those living in rural areas, and only 53% for Americans sixty-five and older.[196] Unless efforts are made to make smartphone access more widely available, millions of Americans could be left out of contact tracing programs.

Second, some groups may bear disproportionate costs of digital disease surveillance. Here it is useful to distinguish between primary and secondary over-surveillance. Primary over-surveillance occurs when certain groups are subject to more surveillance-based disease control than are other groups (relative to disease prevalence across groups).[197] Some public health measures—for example, quarantine or isolation—can have strongly coercive or stigmatizing effects, and there is a long history of disease control being used as a form of social control of minorities and the poor.[198]

---

195. As Sunstein observes, this benefit is "agnostic on large issues of the right and the good" and thus does not presuppose any particular view on difficult questions like the appropriate level of risk tolerance or the comparative value of lives (e.g., as between the young and old or rich and poor). Cass R. Sunstein, *Cognition and Cost-Benefit Analysis*, 29 J. LEGAL STUD. 1059, 1061 (2000).

196. *Mobile Fact Sheet*, *supra* note 72.

197. *See, e.g.*, Wendy K. Mariner et al., *Pandemic Preparedness: A Return to the Rule of Law*, 1 DREXEL L. REV. 341, 354–55 (2009) (describing how people of Chinese ancestry in San Francisco in 1900 were subjected to more extreme vaccination and quarantine procedures despite not being more susceptible to bubonic plague).

198. *See id.* at 358–59 ("[C]oercive measures invite abuse and exacerbate social divisions. Measures like quarantine, surveillance, and behavior control have historically been targeted at people who are already disadvantaged, those on the margins of society, especially immigrants, the poor, and people of color."); *see also* Ashley Southall, *Scrutiny of Social-Distance Policing as 35 of 40 Arrested Are Black*, N.Y. TIMES (Nov. 30, 2020), https://www.nytimes.com/2020/05/07/nyregion/nypd-social-

Marginalized groups may also be subject to secondary over-surveillance, if the data that is collected under the guise of disease prevention is used more broadly. Pretextual and excessive criminal enforcement against racial minorities is a pervasive problem, and, absent strict controls on how digital disease surveillance data is used,[199] may only get worse.

For all these reasons, digital disease surveillance programs need to be carefully designed with fairness in mind.[200] At the same time, fairness concerns may require particularly *aggressive* digital disease surveillance of traditionally marginalized communities. For example, coronavirus, like infectious disease generally,[201] disproportionately harms minority groups,[202] who are more exposed to the disease (because of service-sector jobs that cannot be performed from home), have

---

distancing-race-coronavirus.html (explaining that some elected officials think police officers in New York City are over-enforcing social distancing rules in Black and Hispanic neighborhoods).

199. *See infra* Section III.B.1.

200. *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://www.lawfareblog.com/importance-equity-contact-tracing [https://perma.cc/HG73-CLA2] (proposing recommendations on how to address equity problems that arise with technology-aided tracing, such as operating on an opt-in basis and keeping technology off-limits for law enforcement use).

201. *See* Philip Blumenshine et al., *Pandemic Influenza Planning in the United States from a Health Disparities Perspective*, 14 EMERGING INFECTIOUS DISEASES 709, 710–11 (2008) (describing how a pandemic caused by an influenza virus will result in disparities because of differences in exposure, susceptibility, and treatment between different population groups).

202. *Health Equity Considerations and Racial and Ethnic Minority Groups*, CDC (Feb. 12, 2021), https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/racial-ethnic-minorities.html [https://perma.cc/LW47-DHKC]; *see also* Erin K. Stokes et al., *Coronavirus Disease 2019 Case Surveillance—United States, January 22–May 30, 2020*, 69 MORBIDITY & MORTALITY WKLY REP. 759, 763 (2020) ("Among cases with known race and ethnicity, 33% of persons were Hispanic, 22% were [B]lack, and 1.3% were [non-Hispanic American Indian or Alaska Native]. These findings suggest that persons in these groups, who account for 18%, 13%, and 0.7% of the U.S. population, respectively, are disproportionately affected by the COVID-19 pandemic."). On the unequal impact of coronavirus in general, see Emily A. Benfer et al., *Health Justice Strategies to Combat the Pandemic: Eliminating Discrimination, Poverty, and Health Disparities During and After COVID-19*, 19 YALE J. HEALTH POL'Y, L., & ETHICS 122, 133–36 (2020).

higher rates of preexisting conditions that exacerbate coronavirus, and have worse access to healthcare once they do get sick.[203]

The tension between excessive and insufficient digital disease surveillance is an example of the "discriminatory dualism" that exists throughout society, from policing to housing policy to anti-harassment measures in employment.[204] In all of these cases, marginalized groups suffer from both too much and not enough state intervention. Although this unfortunate dynamic can certainly be improved, it is possible that it can never be fully solved, if only because the underlying social problems are "wicked": there is no agreement on the ultimate goals, information is uncertain and diffuse, and the problem cannot be fully or permanently solved.[205] But even if wicked problems can never be eliminated, they can be continuously managed, as long as policymakers recognize their importance and prioritize their management.

B. Institutional Design

1. Use restrictions

Arguably the most important privacy and civil-liberty safeguard for a digital disease surveillance program is a comprehensive set of use restrictions: rules that govern how collected information can be used, by whom, and for what purposes.[206] As Gostin and Wiley observe,

---

203. Ruqaiijah Yearby & Seema Mohapatra, *Law, Structural Racism, and the COVID-19 Pandemic*, 7 J.L. & BIOSCIENCES 1, 2 (2021).

204. *See generally* Sarah L. Swan, *Discriminatory Dualism*, 54 GA. L. REV. 869, 872–73 (2020) (explaining how in discriminatory dualism "two seemingly contradictory practices . . . come together to form a remarkably durable system of oppression").

205. *See* Alan Z. Rozenshtein, *Wicked Crypto*, 9 U.C. IRVINE L. REV. 1181, 1190–92, 1196–97 (2019) (expanding on the features of "wickedness").

206. The literature on use restrictions in surveillance law is small but growing. *See, e.g.*, ORIN S. KERR, USE RESTRICTIONS AND THE FUTURE OF SURVEILLANCE LAW, BROOKINGS (Apr. 19, 2011), https://www.brookings.edu/research/use-restrictions-and-the-future-of-surveillance-law [https://perma.cc/P492-7CSY] (claiming that "[t]he future of surveillance is a future of use restrictions"); Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 580 (2017) (arguing that the Fourth Amendment should regulate both information use and collection because collection rules cannot address threats that come "solely from information use"); Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 136 (2017) (showing that scholars and courts are beginning to develop use restrictions on lawfully collected information); Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 GEO. MASON L. REV. 412, 412 (2018) (stating that the Fourth Amendment can and

"[h]ealth information can reveal intimate details that may adversely affect an individual's employment, child custody, immigration status, insurance, or public benefits."[207] Thus, use restrictions must address whether data can be used for purposes not immediately connected to public health. This is especially true for location data, which could be relevant for criminal investigations or immigration enforcement.

The importance of use restrictions is reflected in their close connection to the one factor that regularly plays a decisive role in special-needs analysis: whether the surveillance is for traditional law enforcement purposes.[208] Use restrictions pick up where that inquiry ends: even if a program is not designed for law enforcement purposes, if the data that is collected is regularly used for such purposes, the same privacy and civil liberties concerns are implicated.

There are several justifications for use restrictions. First, people may be more willing to comply with disease surveillance if they know that their information will not be used to subject them to criminal or immigration consequences. Second, the greater the limitations on the use of information, the less likely it is to be abused. Third, it is only for the most serious of offenses that maximum enforcement is socially desirable, and a key way that enforcement levels are regulated is through the availability of data and other investigative resources for enforcement agencies. A massive influx of data from an unrelated program can upset that balance and lead to over-enforcement.

Although use restrictions are not a central feature of American surveillance law, they are not unknown to it either. Lower courts have made limited attempts to impose use restrictions under the Fourth Amendment,[209] but the Supreme Court has generally declined to

---

should regulate the use of lawfully collected information). An early proposal for use restrictions is Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995).

207. GOSTIN & WILEY, *supra* note 11, at 307.

208. *See supra* note 152 and accompanying text.

209. For example, the Second Circuit initially held that the Fourth Amendment was violated where the government kept the records of a hard drive for years and then used it as evidence for a different investigation. United States v. Ganias, 755 F.3d 125, 138 (2d Cir. 2014). It later vacated that opinion on rehearing en banc, holding instead that the evidence was admissible under the good faith exception (and thus not reaching the underlying Fourth Amendment issue). United States v. Ganias, 824 F.3d 199, 208–09 (2d Cir. 2016). Another example is *In re Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, in which the magistrate

impose such use restrictions,[210] and so the most important use restrictions are statutory.

The most far-reaching of these statutory restrictions is on census data, which cannot, under any circumstances, be shared outside the Department of Commerce, even for law enforcement purposes.[211] A small exception is made for disclosure in aid of historical research, but even here the law prohibits disclosure of a census's data before seventy-two years after the census is taken.[212]

Another important statutory use restriction is on taxpayer return data, which the Internal Revenue Service cannot generally share with other parts of the government for non-tax-administration purposes.[213] Additional (albeit weaker) use restrictions are found in the foreign intelligence context.[214]

---

judge imposed a variety of use restrictions on cellphone metadata obtained by use of a cell-site simulator. No. 15-M-0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015). For more examples, see Simmons, *supra* note 206, at 180.

210. Simmons, *supra* note 206, at 179. Rebecca Lipman makes the intriguing argument that a case like *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), in which the Court struck down a program that drug tested pregnant women and then shared that information with police, is best understood as implicitly imposing a use restriction (i.e., not to share drug-testing information with police), since, "[w]ithout law enforcement's involvement, the policy would not have been unconstitutional" and "the only part of the policy the Court found objectionable was the sharing of results with law enforcement." Lipman, *supra* note 206, at 450–51.

211. 13 U.S.C. § 9(a); *see also The 2020 Census and Confidentiality*, U.S. CENSUS BUREAU (Jan. 1, 2020), https://www.census.gov/library/fact-sheets/2019/dec/2020-confidentiality.html [https://perma.cc/Y5GC-TS8Q] (explaining that there are no exceptions to the rule that census answers cannot be used for law enforcement purposes).

212. 44 U.S.C. § 2108(b); *see also The "72-Year" Rule*, U.S. CENSUS BUREAU (Dec. 17, 2020), https://www.census.gov/history/www/genealogy/decennial_census_records/the_72_year_rule_1.html [https://perma.cc/Q82T-7CUC] (providing information about the history of the 72-Year Rule).

213. 26 U.S.C. § 6103(a); *see also* Simmons, *supra* note 206, at 183 (explaining that the government applies a use restriction to information disclosed for tax purposes).

214. *See* 50 U.S.C. § 1804(a) (stating that a Foreign Intelligence Surveillance Act (FISA) order can only be obtained if "a significant purpose of the surveillance is to obtain foreign intelligence information"); *id.* § 1806 (imposing a variety of limitations on how FISA information can be used in a criminal case); *see also* Simmons, *supra* note 206, at 183 (arguing that the FISA rules are more lenient than surveillance rules for criminal investigations). One of the most important debates currently being held on FISA reform is over a potential use restriction: banning the government's practice of querying databases of foreign intelligence for information about U.S. persons. *See*

Existing law suggests several models for use restrictions. The simplest and most far-reaching is a census-style blanket ban on unrelated use, which has the benefits of easy administrability and maximum privacy protection. Such a ban has been proposed in the Senate, suggesting some degree of political support.[215] The main disadvantage of such a ban is that it has no exceptions either for serious crimes or the prevention of imminent harm.[216]

If policymakers decide that a blanket ban is excessive, there are several ways of imposing more limited use restrictions. The weakest form would be procedural restrictions, such as high-level certifications by requesting agencies or court review.[217] The next level up would be an explicit list of offenses, investigations of which would permit enforcement agencies to get digital disease surveillance data.[218] This approach has the benefit of allowing for narrow tailoring, although the experience of the Wiretap Act, which explicitly lists those offenses for which real-time electronic surveillance is permitted, is not encouraging: the Wiretap Act's list is twenty-one subsections long and lists dozens of offenses.[219]

If a blanket ban is rejected, the best approach would be to impose a high general standard on when information can be shared. For

---

Elizabeth Goitein & Robert S. Litt, *A Way Forward on Section 702 Queries*, LAWFARE (Feb. 20, 2018, 12:30 PM), https://www.lawfareblog.com/way-forward-section-702-queries [https://perma.cc/TS59-XP67] (suggesting five changes to FISA procedures that would increase accountability). The Second Circuit has held that querying is a separate Fourth Amendment event from collection and thus must meet the general requirement of Fourth Amendment reasonableness. United States v. Hasbajrami, 945 F.3d 641, 670 (2d Cir. 2019).

215. Public Health Emergency Privacy Act, S. 3749, 116th Cong. § 3(a)(4) (2020) (permitting disclosure, including by a government entity, of individually identifiable coronavirus data to a government entity only "when the disclosure . . . is to a public health authority; and . . . is made . . . solely for good faith public health purposes and in direct response to exigent circumstances").

216. *Id.*

217. *See, e.g.*, Krent, *supra* note 206, at 87–88 (describing how the warrant requirement is intended to constrain government officials by requiring them to declare the purpose and aim of a search before it takes place).

218. *See id.* at 82–83 (showing how Congress has limited an agency's authority to disclose information under the Privacy Act to cases where the individual consents, or for "routine uses" of information, civil or criminal law enforcement purposes, census-related activities, and other specified purposes).

219. *See* 18 U.S.C. § 2516(1) (listing twenty-one subsections of offenses, ranging from aircraft piracy to illegal monopolies).

example, the Stored Communications Act permits communication services to voluntarily share the contents of their user's information with law enforcement when "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 communications relating to the emergency."[220]

2. Ex ante oversight

Surveillance programs are generally judicially reviewable ex post: an aggrieved party can challenge surveillance that has already taken place.[221] Unfortunately, ex post review has well-known drawbacks. Courts are often loathe to second-guess decisions made by executive-branch officials. Courts are also subject to loss aversion, whether in terms of stopping a surveillance program that is providing useful information or, in the case of a criminal trial, suppressing evidence derived from the surveillance.[222] In other words, when the government asks for forgiveness rather than permission, it often gets both.

For this reason ex ante authorization is generally considered the gold standard for judicial oversight.[223] One benefit of ex ante authorization is that it puts the reviewing magistrate in charge of the ultimate determination as to the appropriateness of surveillance, and it is more likely that the equities at stake—not just safety but also privacy and civil liberties—will be better balanced by a "neutral and detached" magistrate than by a government "officer engaged in the often competitive enterprise of ferreting out crime"[224] or, in this case, disease. And even where judges approve most surveillance requests

220. *Id.* § 2702(b)(8).

221. *See, e.g.*, *id.* § 2707(a) (providing for civil remedies in Stored Communications Act cases).

222. *See, e.g.*, United States v. Ozar, 50 F.3d. 1440, 1448 (8th Cir. 1995) (holding that even where a surveillance program inadvertently collected privileged communications, those communications would only be suppressed if the defendant could prove they were privileged because there was no showing of bad faith); *see also* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1611, 1622 (2012) (arguing that courts do not often suppress evidence in criminal cases).

223. *See* Bar-Gill & Friedman, *supra* note 222, at 1647 (explaining how an ex ante warrant model removes the problem of judicial bias and is therefore preferrable); David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425, 479–81 (2016) (discussing how the warrant requirement's ex ante review is beneficial).

224. Johnson v. United States, 333 U.S. 10, 14 (1948).

(and thus appear to be little more than "rubber stamps"), the mere requirement of having to justify a surveillance request has a disciplining effect on the government.[225]

It is important to separate the timing of oversight from its substance. Support for ex ante review does not imply support for any particular standard of review, for example, probable cause. In fact, there is legislative precedent for ex ante oversight coupled with a spectrum of review standards.[226] For example, federal wiretap law requires the reviewing court to establish factors that go beyond probable cause, like necessity,[227] and only permits wiretaps for investigation of certain particularly serious offenses.[228] By contrast, the Stored Communications Act allows the government to compel the production of certain types of electronic data as long as "there are reasonable grounds to believe that the [information sought is] . . . relevant and material to an ongoing criminal investigation."[229] And section 702 of the Foreign Intelligence Surveillance Act (FISA) of 1978 requires ex ante judicial oversight of programs rather than of specific targets.[230]

3. Procedures to limit discretion

Designing a rights-protective surveillance regime is not simply a matter of ensuring that surveillance is not excessive; the surveillance must also not be *arbitrary*. Starting with colonial resistance to writs of assistance, which allowed British officials to require American law enforcement officials to help search any house for smuggled goods,[231]

---

225. *See, e.g.*, Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 IND. L.J. 1191, 1229 (2016) (arguing that high rates of approval result because Justice Department lawyers are meeting standards, not because judges are operating as rubber stamps); Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?: Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125, 128–29 (2014) (arguing that there are so few rejections because the government only brings cases in the ex parte context when it is reasonably sure it can win).

226. There is also judicial precedent for this approach, see *Camara v. Municipal Court*, 387 U.S. 523, 534–35, 539 (1967), though the court quickly abandoned that approach in *Terry v. Ohio*, 392 U.S. 1, 27 (1968).

227. 18 U.S.C. § 2518(1)(c).

228. *Id.* § 2516.

229. *Id.* § 2703(d).

230. *See* 50 U.S.C. § 1881a (describing FISA's judicial oversight procedures).

231. Massachusetts revolutionary James Otis famously denounced writs of assistance as the "worst instrument of arbitrary power, the most destructive of English liberty," because they "place[d] the liberty of every man in the hands of every petty officer."

courts and commentators have long recognized arbitrariness as one of (if not the chief) evil that the Fourth Amendment was meant to address.[232] This concern is most apparent in the Fourth Amendment's requirement that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized."[233]

But where the warrant requirement does not apply, the Court has nevertheless looked to procedural substitutes to prevent arbitrariness, either through clear statutory guidelines or, as relevant here, administrative rules and regulations.[234] Thus, in its early administrative-search cases, the Court emphasized that warrantless, suspicionless searches required clear guidelines and procedures to pass constitutional muster.[235] Similarly, the Fourth Amendment's inventory exception, which authorizes warrantless, suspicionless searches of arrestees and their possessions, has always been justified in part on "standardized procedures ensuring that officers did not make discretionary decisions to search."[236]

Detailed procedures are especially important where data can be used for multiple purposes. Disease surveillance data can be used not only for the prevention of disease, but also for various law enforcement purposes. As noted above, a key feature of the Fourth Amendment's special-needs doctrine is that data not be collected for traditional law

---

JAMES OTIS, AGAINST WRITS OF ASSISTANCE (Feb. 1761), (transcript available at http://www.nhinet.org/ccs/docs/writs.htm [https://perma.cc/C8MQ-F8XJ]).

232. *See* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1722 (2014) [hereinafter Slobogin, *Panvasive Surveillance*] (describing the scholarly consensus that the Fourth Amendment was meant to prohibit general warrants that authorized "random and undifferentiated" searches during colonial times).

233. U.S. CONST. AMEND. IV.

234. As Slobogin notes, much of administrative law is a "stand-in[] for the moribund non-delegation doctrine," including in particular the requirement that "any rules that are promulgated have a reasonable, explicit basis that is made apparent to the public." Slobogin, *Panvasive Surveillance*, *supra* note 232, at 1759–60.

235. *See, e.g.*, Donovan v. Dewey, 452 U.S. 594, 604–05 (1981) (holding that since the Federal Mine Safety and Health Act of 1977 provided a predictable and guided federal regulatory presence, the warrantless searches were constitutional); United States v. Biswell, 406 U.S. 311, 315–16 (1972) (finding that warrantless regulatory inspections under a statute that were carefully limited in time, place, and scope were constitutional); *see also* Primus, *supra* note 136, at 269–70 (arguing that when the Court found warrantless regulatory searches constitutional in early cases, it required other limits on executive discretion).

236. Primus, *supra* note 136, at 304.

enforcement purposes.[237] Clear guidelines regulating what data is collected, how it may be collected (including from private entities), and how it may be used is an important way of ensuring that this requirement is satisfied.

The obvious model for proceduralizing disease surveillance is the rulemaking process that is prevalent throughout the regulatory state. Although administrative rulemaking is not a common feature of American surveillance regimes in the contexts of law enforcement and foreign intelligence,[238] it is generally applicable to public health surveillance.[239] And even where federal or state administrative-procedure statutes do not apply, their underlying logic of notice-and-comment rulemaking could be used to proceduralize surveillance programs.[240] Of course, public-rulemaking requirements should be tempered with exceptions for interim and immediate action, as already exist under federal administrative law.[241]

4. Surveillance hygiene

Whether imposed by law or agency procedure, minimization procedures (to ensure that only relevant data is collected), retention policies (to regulate how long and how data may be retained by the government), and information-security practices (to ensure that data is not improperly disclosed or altered) are a part of any well-designed surveillance system. Call it "surveillance hygiene": the background processes applicable to any surveillance program, no matter its subject

237. *See supra* note 152 and accompanying text.

238. *See supra* note 178 and accompanying text.

239. *See, e.g.*, Control of Communicable Diseases; Foreign Quarantine, 85 Fed. Reg. 7874–86 (Feb. 12, 2020) (to be codified at 42 C.F.R. pt. 71) (justifying increased surveillance for combatting COVID-19 and explaining that such surveillance has always been a part of disease control).

240. *See, e.g.*, Friedman & Ponomarenko, *supra* note 178, at 1834 (arguing that policing can be governed by democratic authorization such as notice-and-comment rulemaking with public participation); Renan, *supra* note 172, at 1092–93 (asserting that administrative law and agency lawmaking can provide a framework for surveillance); Slobogin, *Panvasive Surveillance*, *supra* note 232, at 1751–55 (discussing how legislative and representative authorization could play a rule in fusion centers, closed circuit camera surveillance, and drone use).

241. *See* 5 U.S.C. § 553(b) (permitting an agency to skip notice and comment procedures "when the agency for good cause finds . . . that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest").

area, that operate day in and out to ensure smooth and privacy-protective functioning.

Surveillance-hygiene requirements are scattered throughout the surveillance state, though unfortunately usually not in a comprehensive fashion. In the criminal context, the most important example is the federal Wiretap Act, which requires that recorded communications be protected from alteration, be retained for at least ten years,[242] and "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[243] Foreign-intelligence surveillance gathered in the United States is similarly subject to proper targeting and minimization rules.[244] In both cases, the statutes' requirements are further developed in internal regulations, some of which are publicly available.[245]

Fortunately, at least some policymakers have already recognized the need for such policies with digital disease surveillance. For example, draft legislation introduced by Senate Democrats would require government entities (though inexplicably not public-health authorities themselves) to ensure the "security and confidentiality of emergency health data"[246] (an important requirement given the vulnerability of digital disease surveillance to hackers and foreign intelligence agencies[247]) and to delete data after the health crisis is over.[248]

---

242. 18 U.S.C. § 2518(8)(a).

243. *Id.* § 2518(5).

244. 50 U.S.C. §§ 1881a(c)(1)(A), (d), (e). Targeting procedures ensure that surveillance is limited to only those individuals that can lawfully be surveilled, and minimization procedures ensure that information that is irrelevant or incidentally acquired information is not disseminated.

245. For law-enforcement wiretaps, see DEP'T OF JUST., ELECTRONIC SURVEILLANCE MANUAL ii (2005). For minimization procedures for foreign-intelligence surveillance under Section 702 of FISA, see *Release of 2015 Section 702 Minimization Procedures*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.intel.gov/index.php/ic-on-the-record-database/results/6-release-of-2015-section-702-minimization-procedures [https://perma.cc/2U27-LPY2].

246. Public Health Emergency Privacy Act, S. 3749, 116th Cong. § 3(b) (2020).

247. *See* Natasha Singer, *Virus-Tracing Apps Are Rife with Problems. Governments Are Rushing to Fix Them*, N.Y. TIMES (July 20, 2020), https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html (describing virus tracing apps that resulted in leaks of users' private information in Qatar and India).

248. Public Health Emergency Privacy Act, S. 3749, 116th Cong. § 3(g) (2020).

5. Ex post oversight

Once a disease surveillance program is up and running, it should be subject to multiple and ongoing levels of review, both to ensure that the surveillance is being undertaken in a lawful way and that the relevant procedures are periodically updated to take into account changing circumstances. This review could come in many forms, both inside and outside the surveillance agency. Current surveillance programs offer numerous examples. For example, inspectors general[249] and compliance offices[250] could operate inside disease surveillance agencies.[251] Review could also come from other agencies, following the model of the Privacy and Civil Liberties Oversight Board (PCLOB), which reviews terrorism surveillance programs.[252] Review could also come from other government branches, whether the judiciary (in the form of periodic review of ongoing programs) or the legislature (in the form of reporting to relevant legislative committees).

---

249. *See* Shirin Sinnar, *Protecting Rights from Within?: Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027, 1027, 1031 (2013) (showing that inspectors general have the capacity to provide transparency and identify violations of the law).

250. *See* Shirin Sinnar, *Institutionalizing Rights in the National Security Executive*, 50 HARV. C.R.-C.L. L. REV. 289, 301–02, 306–09 (2015) (using the Department of Homeland Security Office for Civil Rights and Civil Liberties (CRCL) as an example of a compliance officer charged with examining the Department's own actions for First Amendment concerns).

251. The Department of Health and Human Services already has an inspector general, whose responsibility covers the Centers for Disease Control (CDC), the nation's primary disease surveillance agency. *See* Dep't of Health & Hum. Serv. Off. of Inspector Gen., *HHS-OIG Strategic Plan 2020–2025*, 4 (2020); *Mission, Role and Pledge*, CTRS. DISEASE CONTROL & PREVENTION (May 13, 2019), https://www.cdc.gov/about/organization/mission.htm [https://perma.cc/R8MF-Z4XY].

252. *See* Sinnar, *supra* note 250, at 316–21 (describing the development and role of the PCLOB, including its report on NSA phone records, which prompted substantial changes to the program); Renan, *supra* note 172, at 1118–23 (describing the PCLOB as part of a gradual evolution toward an effective framework for "programmatic efficacy review" and suggesting steps for further development). Encouragingly, the Board's chair and one of its members published an op-ed applying lessons from post-9/11 surveillance to digital disease surveillance. This shows both the Board's interest and the sort of expertise it could bring to bear. *See* Adam Klein & Edward Felten, *The 9/11 Playbook for Protecting Privacy*, POLITICO (Apr. 4, 2020, 11:11 AM), https://www.politico.com/news/agenda/2020/04/04/9-11-playbook-coronavirus-privacy-164510 [https://perma.cc/92F2-JHQZ] (outlining suggestions on how to implement post-9/11 PCLOB policies in the context of the pandemic).

6. Transparency

All of the institutional-design features described above can be implemented in a more or less transparent way. In the context of law enforcement or national security surveillance, it is difficult to get the level of transparency right. Too much transparency can undermine a surveillance program's effectiveness if it helps the targets of the program evade it. But too little transparency undermines democratic accountability and can lead to abuse. Thus, transparency regimes for traditional surveillance programs have always been half-a-loaf measures. For example, the Wiretap Act requires that the target of a wiretap be notified, but notification can be delayed during the pendency of the investigation.[253] And foreign intelligence and national security programs have the added burden of being conducted under strict classification regimes, which makes public reporting and accountability especially challenging.

Fortunately, these challenges are largely absent in the disease surveillance context. Although some of the underlying surveillance data—specifically, personally identifiable information—should not be publicly disclosed, the details of how a disease surveillance program actually operates can and should be made public. To the extent that disease surveillance programs operate in partnership with private companies, these companies could—either voluntarily or through legal mandates—provide public "transparency reports" outlining what information they have collected and provided to the government.[254]

Although a small minority of individuals may use this information to evade surveillance, most people will likely not modify their behavior even if they know how the program operates (especially since evasion would require costly practices like not carrying around a smartphone). Thus, all of the institutional safeguards described above—ex ante review by judges, administrative rulemaking, and ex post review—can and should be done in a maximally transparent manner.

C. Democratic Authorization

The more far-reaching a disease surveillance program is, the more precisely its contours should be set in advance by legislative authorization.

---

253. 18 U.S.C. § 2518(8)(d).

254. These companies already do this for law enforcement requests. Rozenshtein, *supra* note 174, at 146–48.

This "principle of legality," as it is known outside the United States,[255] has at least two distinct sources in the Constitution.

The first source is the Fourth Amendment itself. The Supreme Court's initial special-needs cases emphasized the importance of clear legislative standards.[256] For example, *in Camara v. Municipal Court of the City and County of San Francisco*,[257] the Court's first major Fourth Amendment reasonableness case, the Court observed that "probable cause to issue a warrant to inspect must exist if reasonable *legislative* or administrative standards for conducting an area inspection are satisfied."[258] And in *Donovan v. Dewey*,[259] the Court approved of a warrantless inspection regime on the grounds that legislation "establishe[d] a predictable and guided federal regulatory presence."[260]

Over the past several decades the Court has moved away from its emphasis on legislative authorization as a key component of Fourth Amendment reasonableness.[261] But it should not be difficult to resurrect this thread of the doctrine. Reasonableness, after all, is "a term literally crying out for balance between the competing interests

---

255. Invoking the principle of legality, in April 2020 the Israeli Supreme Court held that the Israeli government must secure implementing legislation in the Knesset (Israel's legislature) in order to use the domestic intelligence agency, the Shin Bet (roughly equivalent to America's FBI), for coronavirus-related surveillance. Elena Chachko, *The Israeli Supreme Court Checks COVID-19 Electronic Surveillance*, LAWFARE (May 5, 2020, 1:10 PM), https://www.lawfareblog.com/israeli-supreme-court-checks-covid-19-electronic-surveillance [https://perma.cc/RY4D-7RWF]. In response the Israeli Knesset authorized such surveillance. *See* Amir Cahane, *Israel Reauthorizes Shin Bet's Coronavirus Location Tracking*, LAWFARE (July 3, 2020, 9:40 AM), https://www.lawfareblog.com/israel-reauthorizes-shin-bets-coronavirus-location-tracking [https://perma.cc/NPQ7-NG74] (discussing legislation enacting temporary provisions re-tasking the Shin Bet with coronavirus tracking); *see also* Ben Emmerson, (Special Rapporteur), Hum. Rts. Council, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, ¶36, U.N. Doc A/HRC/34/61 (Feb. 21, 2017).

256. Primus, *supra* note 136, at 269–70; *see supra* notes 136–53 and accompanying text (discussing the development of special-needs doctrine and how the combination of two lines of cases created an unclear standard).

257. 387 U.S. 523 (1967).

258. *Id.* at 538 (internal quotation marks omitted and emphasis added).

259. 452 U.S. 594 (1981).

260. *Id.* at 603–04.

261. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117, 1121–22 (2017) ("Structural differences between the Fourth Amendment and investigative legislation make legislation a poor signal of constitutionally relevant judgments.").

of individual privacy and societal security."[262] Who better to do so than the legislature, the most democratically accountable of the branches of government?

The second source is the non-delegation doctrine, which has already been used in a major state court case to invalidate a coronavirus lockdown.[263] In its canonical formulation, the non-delegation doctrine requires that the legislature provide an "intelligible principle" when delegating power so as to guide the exercise of executive discretion.[264] At the state level the non-delegation doctrine has had a more direct effect and has routinely been used to strike down surveillance activities that have no legislative authorization.[265] At the federal level, although the Supreme Court has only struck down legislation on non-delegation grounds twice (both times in 1935, at the height of the Supreme Court's resistance to the New Deal[266]), the non-delegation doctrine has continued to play an important role in judicial review of federal legislation through the doctrine of constitutional avoidance, whereby expansive statutes are construed narrowly so as to avoid potential non-delegation problems.[267] Perhaps most importantly, *Gundy v. United States*[268] suggests that there is a potential majority on the Supreme Court in favor of bringing back a substantive non-delegation doctrine.[269]

---

262. United States v. Graham, 824 F.3d 421, 439 (4th Cir. 2016) (en banc) (Wilkinson, J., concurring); *see also* Rozenshtein, *supra* note 116, at 956–57 (describing the structural advantages legislatures have in investigating complex constitutional issues).

263. *See* Wis. Legislature v. Palm, 942 N.W.2d 900, 912–13 (Wis. 2020) (invalidating Wisconsin's lockdown order in part because construing the relevant statute as permitting the lockdown would raise a serious question as to its constitutionality under the state non-delegation doctrine).

264. J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928).

265. Friedman & Ponomarenko, *supra* note 178, at 1893–94.

266. *See* A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495, 529–32, 551 (1935) (determining that Congress overstepped its limits); Panama Refin. Co. v. Ryan, 293 U.S. 388, 414–15, 420, 430 (1935).

267. *See* John F. Manning, *The Nondelegation Doctrine as a Canon of Avoidance*, 2000 SUP. CT. REV. 223, 242–43 (2000) (stating that judges incorporate the doctrine of non-delegation indirectly by using the canon of avoidance).

268. 139 S. Ct. 2116 (2019).

269. *Id.* at 2130–31 (Alito, J., concurring in the judgment); *id.* at 2131 (Gorsuch, J., dissenting). Justice Kavanaugh did not participate in *Gundy*, but his subsequent opinions have signaled sympathy with the *Gundy* dissenters. *See* Paul v. United States, 140 S. Ct. 342, 342 (2019) ("Justice Gorsuch's scholarly analysis of the Constitution's

There are also good policy reasons to favor legislative involvement. Legislatures can provide an important counterweight to executive power. Legislatures can enhance democratic participation by offering a forum for interest groups to make their interests heard,[270] which is especially important where, as is the case with disease surveillance, there is a risk that costs and benefits will not be distributed equitably across society.[271] Legislative authorization can also increase compliance with public-health responses, since such authorization is an important way that government action is legitimated.[272] And, especially if legislation includes sunset clauses—provisions that cancel a government program unless the legislature explicitly reauthorizes it by a certain date—it can force both legislatures and executive agencies to continuously update digital disease surveillance programs to reflect changing circumstances.[273]

IV. THE ROLE OF COURTS

We can now revisit the question raised at the end of Part II: given that current Fourth Amendment doctrine—specifically the special-needs exception—imposes few real limits on the government's ability to engage in digital disease surveillance, should it be updated? As Part III demonstrated, there are many additional safeguards that can be implemented that do not interfere with program effectiveness.

I believe that courts should modify Fourth Amendment doctrine to require at least some of these safeguards. This is in large part a normative hope, but there is also precedent for this kind of doctrinal evolution. As Professor Orin Kerr has explained, a key meta-narrative in Fourth Amendment law is "equilibrium adjustment," by which courts modify Fourth Amendment doctrine to respond on the one

---

nondelegation doctrine in his *Gundy* dissent may warrant further consideration in future cases.").

270. As Slobogin notes, "delegations [that] surrender the legislative power to the executive branch . . . are a recipe for uneven application of the law." Slobogin, *Panvasive Surveillance*, *supra* note 232, at 1744.

271. *See supra* Section III.A.2.

272. On the importance of perceived legitimacy to compliance with government policy, see generally TOM R. TYLER, WHY PEOPLE OBEY THE LAW 3–6 (1990).

273. *See generally* Jacob E. Gersen, *Temporary Legislation*, 74 U. CHI. L. REV. 247, 266–67 (2007) (discussing the main informational benefits of temporary legislation: optimal public policy, diminished cognitive bias, and mitigation of asymmetric information in politics).

hand to new public safety threats (by relaxing Fourth Amendment rules) and on the other hand to increased government-surveillance capabilities (by strengthening Fourth Amendment rules).[274]

In Section A, I outline three principles that should guide courts in how they apply the Fourth Amendment to digital disease surveillance programs. In Part B, I zoom out from the issue of disease surveillance and argue that the principles learned from that context can usefully be applied to the challenge of updating Fourth Amendment doctrine for digital surveillance generally.

A. Deference, Patience, and Flexibility

At its core, the issue of judicial review of digital disease surveillance implicates "the central (and long-running) normative debate over emergency powers: Should constitutional constraints on government action be suspended in times of emergency . . . or do constitutional doctrines forged in calmer times adequately accommodate exigent circumstances?"[275] Precedent fails to provide clear answers: for every case permitting emergency powers, one can find a case rejecting them.[276] Nor does history provide easy answers. *Korematsu v. United States*,[277] which upheld the World War II internment of Americans of Japanese descent,[278] is one of the most notorious members of the "anticanon" of Supreme Court decisions,[279] while Lincoln's unilateral suspension of habeas corpus, in defiance of the Chief Justice of the United States,[280] is often held up as the canonical example of when

---

274. *See* Kerr, *supra* note 116, at 530–31 (discussing how equilibrium-adjustment allows for adherence to the Fourth Amendment amidst changing facts).

275. Lindsay F. Wiley & Steve Vladeck, *COVID-19 Reinforces the Argument for "Regular" Judicial Review—Not Suspension of Civil Liberties—In Times of Crisis*, HARV. L. REV. BLOG (Apr. 9, 2020), https://blog.harvardlawreview.org/covid-19-reinforces-the-argument-for-regular-judicial-review-not-suspension-of-civil-liberties-in-times-of-crisis [https://perma.cc/N55H-CZ2B].

276. *Compare, e.g.*, Jacobson v. Massachusetts, 197 U.S. 11, 12–13, 39 (1905) (upholding compulsory vaccination in response to a smallpox epidemic), *with, e.g.*, Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 579–80, 582 (1952) (holding that the President did not have inherent power to temporarily take control of a steel plant to ensure the adequate supply of steel during the Korean War).

277. 323 U.S. 214 (1944).

278. *Id.* at 223–24, *abrogated by* Trump v. Hawaii, 138 S. Ct. 2392 (2018).

279. *See generally* Jamal Greene, *The Anticanon*, 125 HARV. L. REV. 379, 456, 459–60, 462 (2011) (discussing *Korematsu*'s role in the anticanon).

280. *Ex parte* Merryman, 17 F. Cas. 144, 148 (C.C.D. Md. 1861) (No. 9487).

unconstitutional actions can be justified by exigent circumstances.[281] And while I of course agree that courts have a critical role to play in ensuring that the government lives up to its civil liberties responsibilities,[282] my view for judicial review includes three important limitations.

First, courts should generally defer to the judgments of the political branches when it comes to unavoidable tradeoffs between privacy and public safety. Where a program is so poorly designed that privacy is being needlessly sacrificed for no safety benefit, it is appropriate for the courts to require that the program be altered. But where the government has attempted in good faith to design a program that is substantively effective and has procedural safeguards, the courts should respect its ultimate judgment as to how much privacy is worth sacrificing for increased safety, especially where the program has been legislatively authorized and where its burdens fall uniformly over the population.[283]

This is a straightforward application of the Legal Process school principle of institutional settlement, "which holds that law should allocate decisionmaking to the institutions best suited to decide particular questions, and that the decisions arrived at by those institutions must then be respected by other actors in the system, even if those actors would have reached a different conclusion."[284] Conditional on the safeguards described in Part III, the question of the optimal level of digital disease surveillance is a policy decision like any

281. As Lincoln argued in the wake of *Merryman*, "[A]re all the laws *but one* to go unexecuted, and the Government itself go to pieces, lest that one be violated?" Abraham Lincoln, *Message to Congress in Special Session*, *in* ABRAHAM LINCOLN: HIS SPEECHES AND WRITINGS 601 (Roy P. Basler ed., 1946).

282. *See, e.g.*, Lindsay F. Wiley & Stephen I. Vladeck, *Coronavirus, Civil Liberties, and the Courts: The Case Against "Suspending" Judicial Review*, 133 HARV. L. REV. F. 179, 182–83, 197–98 (2020) (discussing that courts should not adopt a more deferential standard of review in response to emergencies such as the pandemic); Ram & Gray, *supra* note 9, at 11 (offering a "constitutionally informed framework" as a "guide for courts to evaluate the constitutional sufficiency of the regulatory structures erected around" digital disease surveillance programs).

283. *See supra* Section III.A.

284. Ernest A. Young, *Institutional Settlement in a Globalizing Judicial System*, 54 DUKE L.J. 1143, 1149–50 (2005).

other in a modern regulatory state, a decision that in our constitutional system is primarily addressed to the political branches.[285]

Second, courts should distinguish between short-term and long-term review of digital surveillance programs.[286] Courts should give more leeway when a program is first implemented, given that—especially in times of emergency—it is likely that the program will initially fail to fully implement some or most of the safeguards described in Part III. Courts should recognize this deep uncertainty and preserve a space for experimentation. They should also recognize which safeguards can be implemented immediately (for example, use restrictions and transparency) and which, like detailed procedures based on public input, may require months or even longer to fully implement.

Third, even once best practices are developed, and courts are in a more secure position from which to review surveillance programs, they should go beyond their standard repertoire of remedies, which traditionally are limited to the binary choice of fully approving a program or otherwise striking it down in its entirety. There are a variety of ways in which courts can help the political branches improve the constitutionality of digital disease surveillance. For example, courts could, either through constitutional-avoidance or clear-statement rules, interpret surveillance statutes narrowly, requiring the political branches to address potential constitutional problems with more care.[287] Even where they apply substantive constitutional law and

---

285. *See* Rozenshtein, *supra* note 116, at 956–57 (describing the "several structural advantages" that legislatures have over courts when it comes to "surveillance policymaking").

286. Wiley and Vladeck object to the "suspension" of judicial review because such an approach "is inextricably linked with the idea that a crisis is of finite—and brief—duration. [But] [t]o that end, the principle is ill-suited for long-term and open-ended emergencies like the one in which we currently find ourselves." Wiley & Vladeck, *supra* note 282, at 182; *see also* Ilya Somin, *Judicial Review and Emergency Powers*, JOTWELL (June 29, 2020), https://conlaw.jotwell.com/judicial-review-and-emergency-powers [https://perma.cc/YLC3-TA7N] (agreeing with Wiley and Vladeck). But crisis is not binary, and neither is judicial review. As the crisis gradually recedes, the strength of judicial review can gradually ramp up, and vice versa.

287. *See* Friedman & Ponomarenko, *supra* note 178, at 1894–97 (advocating for the use of clear statement rules, which allow courts to remand cases with constitutional interests not taken into account by Congress or an agency); *see also* Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 1513–15 (2014) (arguing that narrow interpretation would "encourage more transparent and effective surveillance laws").

determine that a surveillance program is unconstitutional, courts could use "suspension[s] of invalidity" to give "a period of time for the government to apply its own fix to a constitutional infirmity before judicial invalidation of an act."[288]

B. The Future of the Fourth Amendment: "Special Needs with Bite"

As I have argued previously, "a critical research agenda in Fourth Amendment scholarship must be to develop an account of what substitutes for warrants are reasonable in a digital age."[289] This is true not just when it comes to digital disease surveillance but also to "emerging 'data driven,' 'big data,' and 'predictive' policing" applied to ordinary law enforcement priorities.[290] "Because these investigative practices rely on accumulating and analyzing large data sets, they cannot operate if the government is required to establish probable cause that a particular individual is tied to a particular offense before the government can collect or analyze that person's data."[291] But if such surveillance is excluded from Fourth Amendment coverage, or (what is functionally equivalent) subject only to a vague and deferential "special needs" analysis that is stacked in favor of the government, then "highly intrusive and privacy-threatening government activity will go unchecked."[292]

This problem cannot be wished away merely by urging courts to value privacy over security, simultaneously expanding the scope of the Fourth Amendment and imposing a strict warrant requirement. Were the federal bench—and the Supreme Court in particular—full of civil

---

288. Greene, *supra* note 186, at 118; *see, e.g.*, N. Pipeline Constr. Co. v. Marathon Pipe Line Co., 458 U.S. 50, 88 (1982) (staying the invalidation of the federal statute granting jurisdiction to bankruptcy courts so as to "afford Congress an opportunity to reconstitute the bankruptcy courts or to adopt other valid means of adjudication, without impairing the interim administration of the bankruptcy laws"); ACLU v. Clapper, 785 F.3d 787, 826 (2d Cir. 2015) (holding that a national-security surveillance program exceeded statutory authorization but declining to enjoin the government from operating it on the grounds that it was to expire in several weeks and the government had "vigorously contend[ed] that the program [was] necessary for maintaining national security, which of course is a public interest of the highest order").

289. Rozenshtein, *supra* note 116, at 960.

290. *Id.* at 951.

291. *Id.*

292. *Id.*

libertarians, we would have noticed by now, and decades of legal scholarship criticizing the courts' narrowing of the Fourth Amendment would have been unnecessary. "If courts have to choose between hamstringing police"—or the government more broadly—"and allowing privacy intrusions to go unchecked, they will likely choose the latter. But the public loses out either way."[293]

What is needed, then, is what we might call *special needs with bite*:[294] a set of doctrinally-imposed safeguards that do not simply replicate the standard Fourth Amendment tool of probable-cause warrants but at the same time ensure that reasonableness review does not devolve into a hyper-deferential hunt for any rational government purpose.[295]

In the scholarly literature, this search for alternate implementation of the Fourth Amendment dates back to the work of legal scholars Kenneth Culp Davis[296] and Anthony Amsterdam[297] in the 1960s and 70s, both of whom tried to import administrative law principles into criminal procedure. This tradition has been revitalized in the past decade by the "new administrativists,"[298] much of whose work was discussed in Part II,[299] who urge the application of administrative law tools like cost-benefit analysis and notice-and-comment rulemaking.[300]

---

293. *Id.*

294. *Cf.* Gayle Lynn Pettinga, *Rational Basis with Bite: Intermediate Scrutiny by Any Other Name*, 62 IND. L.J. 779, 779–80 (1987) (showing how the Supreme Court has previously applied a heightened standard of review while still claiming to use rational basis review).

295. *See* Greene, *supra* note 186, at 118–19 (discussing how flexibility in judicial remedies can lead to more proportionality).

296. *See* KENNETH CULP DAVIS, POLICE DISCRETION 98–99, 167 (1975) (arguing that enforcement policies vary with "the whims of particular officers" and should be replaced with a system of "open selective enforcement"); KENNETH CULP DAVIS, DISCRETIONARY JUSTICE: A PRELIMINARY INQUIRY 5–7, 15 (1969) (stating that administrative agencies have a large role in individual justice, which should be effectuated through discretion within the bounds of rules).

297. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 417–18, 422–23 (1974).

298. *See* Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049, 2059 (2016) (defining new administrativists as proponents of agency centric regulation of law enforcement authority).

299. *See supra* notes 187–91, 240 and accompanying text.

300. *See supra* notes 187–91, 240 and accompanying text.

And it is implicit in recent legal reform efforts like the American Law Institute's "Principles of the Law, Policing" project.[301]

A few lower court decisions give examples of what this kind of approach might look like. For example, in *Naperville Smart Meter Awareness v. City of Naperville*,[302] the Seventh Circuit upheld a municipal program to install "smart" residential electricity meters, which would collect far more information about residents' domestic activities than did traditional meters.[303] While holding that the collection was a Fourth Amendment search (and, because conducted without a warrant, presumptively unreasonable), the court upheld the program on general reasonableness grounds, given its relatively minor privacy intrusion, its substantial benefit for the government, and its minimal potential for use in the criminal process.[304] One can imagine a fuller analysis of the program that would have considered all the safeguards laid out in Part III—for example, whether the city had implemented the program based on legislative authorization or transparent regulation, what ongoing safeguards and monitoring existed for the data, and so on.

Another example of an incipient "special needs with bite" approach is the Ninth Circuit's review, in *United States v. Mohamud*,[305] of section 702 of the Foreign Intelligence Surveillance Act of 1978,[306] which permits the warrantless electronic surveillance within the United States of "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[307] Instead of requiring traditional probable-cause warrants, section 702 "sets up a complex system of ex ante judicial oversight (of targeting and minimization procedures) and ex post internal oversight (through multiple layers of compliance review, both within the intelligence agency itself and from the Department of Justice) to minimize incidental impacts on the privacy of U.S. persons."[308] In other words, it comes closest to realizing

---

301. *Principles of the Law: Policing*, AM. L. INST. ADVISER, http://www.thealiadviser.org/policing [https://perma.cc/3X88-29T7].

302. 900 F.3d 521 (7th Cir. 2018).

303. *Id.* at 524.

304. *Id.* at 525, 528–29.

305. 843 F.3d 420 (9th Cir. 2016).

306. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438–48 (codified as amended at 50 U.S.C. § 1881a); *Mohamud*, 843 F.3d at 437–38.

307. § 1881a(a).

308. Rozenshtein, *supra* note 116, at 957–58.

the full list of safeguards described in Part III.[309] And it was because of these safeguards that the Ninth Circuit upheld section 702's constitutionality.[310]

The Supreme Court has nevertheless dragged its feet on reconceptualizing the Fourth Amendment for modern digital surveillance (rather than simply applying traditional Fourth Amendment rules to modern technology, however awkward the fit). For example, in *Carpenter*, its most recent major Fourth Amendment opinion, the Supreme Court brushed off the argument that the Stored Communication Act (SCA), which provided a judicial process for acquiring communications data that deviated from traditional probable-cause warrants,[311] could nevertheless be "reasonable" for Fourth Amendment purposes.[312]

But this refusal to update Fourth Amendment doctrine—in particular to move away from an exclusive focus on probable-cause warrants as the only rigorous limitation on government surveillance—is unsustainable. A broader goal of this Article has been to argue that a well-designed digital disease surveillance program, along the lines outlined in Part III, can serve as a model for future surveillance programs more broadly, and thus also for what a twenty-first century Fourth Amendment should demand of them.

CONCLUSION

Many—no doubt remembering the post-9/11 expansion of the surveillance state—are understandably pessimistic about the effect of digital disease surveillance on privacy. But just as it is important to

309. This is not to say that it could not be improved, or that it is uncontroversial. Professor Laura Donohue in particular has leveled some of the most comprehensive legal critiques of section 702, arguing that it is in effect a system of general warrants. *See generally* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 204–06 (2015). For a response, see Joel Brenner, *A Review of "The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age" by Laura K. Donohue*, 9 J. NAT'L SEC. L. & POL'Y 631, 633–34, 651 (2018) (book review).

310. *Mohamud*, 843 F.3d at 443–44.

311. *See* 18 U.S.C. § 2703(d) (listing the less stringent requirements the government must show to obtain digital information than would be sufficient to grant a warrant).

312. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018); *see also* Rozenshtein, *supra* note 116, at 954–57 (arguing that *Carpenter* mischaracterized the SCA requirements as weaker than they really are and arguing more broadly that legislative authorization should be given more weight in the Fourth Amendment context).

recognize privacy's value, it is just as important to recognize its limits. A key element of privacy is to control, including by keeping secret, the creation and dissemination of information about one's self,[313] and this element is indeed likely to decline if countries embrace digital disease surveillance to fight infectious disease. But although privacy is a key civil liberty, it is not the only one, just as freedom from government surveillance is not the only freedom. Equally important is the freedom to leave one's home, earn a living, and see loved ones, not to mention the freedom to be free from the fear of disease. We may not be able to maximize all of these values, but we can try to maximize overall welfare—and thus minimize the tradeoffs we have to make—through effective and rights-protective government action.

313. GOSTIN & WILEY, *supra* note 11, at 317.