




Mass surveillance in the age of COVID-19

Natalie Ram ^{†*} and David Gray[‡]

Francis King Carey School of Law, University of Maryland, Baltimore, MD 21201, USA

*Corresponding author. E-mail: nram@law.umaryland.edu

ABSTRACT

Epidemiological surveillance programs such as digital contact tracing have been touted as a silver bullet that will free the American public from the strictures of social distancing, enabling a return to school, work, and socializing. This Article assesses whether and under what circumstances the United States ought to embrace such programs. Part I analyzes the constitutionality of programs like digital contact tracing, arguing that the Fourth Amendment's protection against unreasonable searches and seizures may well regulate the use of location data for epidemiological purposes, but that the legislative and executive branches have significant latitude to develop these programs within the broad constraints of the "special needs" doctrine elaborated by the courts in parallel circumstances. Part II cautions that the absence of a firm warrant requirement for digital contact tracing should not serve as a green light for unregulated and mass digital location tracking. In light of substantial risks to privacy, policy makers must ask hard questions about efficacy and the comparative advantages of location tracking versus more traditional means of controlling epidemic contagions, take seriously threats to privacy, tailor programs parsimoniously, establish clear metrics for determining success, and set clear plans for decommissioning surveillance programs.

KEYWORDS: COVID-19, Fourth Amendment, Population-Level Bioethics, Privacy, Public Health, Surveillance

[†] Natalie Ram is Associate Professor of Law, University of Maryland, Francis King Carey School of Law & Greenwall Faculty Scholar in Bioethics.

[‡] David Gray is Jacob A. France Professor of Law, University of Maryland, Francis King Carey School of Law.

INTRODUCTION:

In China, the government has required residents to download a smartphone app that tracks their movements and assigns them a color (red, yellow, or green) corresponding to their asserted public health risk. These color codes regulate access to “subways, malls, and other public spaces.”¹ The methodology by which an individual is color-coded is opaque, however, and the app “also appears to share information with the police, setting a template for new forms of automated social control that could persist long after the epidemic subsides.”² In South Korea, the government reportedly pushes cell phone alerts about infected individuals, sending detailed information including “credit-card history, with a minute-to-minute record of their comings and goings from various local businesses.”³ That level of detail has led to infected individuals, being identified and suffering harassment. Israel has hastily repurposed mass location data secretly collected for counterterrorism purposes to track potentially infected individuals wherever they go.⁴ Meanwhile, in the United States, North and South Dakota have already issued an app for their residents, which gathers location data using cell towers, GPS, and Wi-Fi and stores those data on a centralized, private server.⁵ In all, according to one live-tracking site, at least 53 contact tracing apps have already appeared across at least 29 countries.⁶

In the United States, the Supreme Court has held that individuals have the right to expect that “the whole of their physical movements” will remain private.⁷ Location data from smartphones and cell phones “provide[] 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.”⁸ Yet the explosive growth of COVID-19⁹ in this country and the drastic social distancing measures that have crippled

1 See Paul Mozur, Raymond Zhong and Aaron Krolik, *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*, N.Y. Times (Mar. 1, 2020), <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>.

2 *Id.*

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

4 David M. Halbfinger, Isabel Kershner & Ronen Bergman, *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*, N.Y. Times (Mar. 18, 2020), <https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html>.

5 See Jennifer Valentino-DeVries, Natasha Singer & Aaron Krolik, *A Scramble for Virus Apps That Do No Harm*, N.Y. Times (Apr. 29, 2020), <https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html>; see also *Care19*, North Dakota, <https://ndresponse.gov/covid-19-resources/care19> (last visited Apr. 30, 2020); *Care19 App*, COVID-19 in South Dakota, <https://covid.sd.gov/care19app.aspx> (last visited Apr. 30, 2020).

6 See Samuel Woodhams, *COVID-19 Digital Rights Tracker*, Top10VPN (Apr. 28, 2020), <https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/>.

7 *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

8 *Id.* (internal quotation marks omitted).

9 COVID-19 is the name for the cluster of symptoms caused by the contagion SARS-CoV-2. In this essay, we use COVID-19 as a generic term to refer both to the disease and the contagion. We embrace this imprecision because COVID-19 is the more widely recognized term, it is commonly used to refer to both disease and contagion, and in order to avoid any potential confusion with SARS-CoV, which first emerged in 2003, and is the cause of disease symptoms commonly referred to as SARS. See Ctrs. for Disease Control (CDC), *Severe Acute Respiratory Syndrome (SARS)* (Dec. 6, 2017), <https://www.cdc.gov/sars/index.html>.

American life and the economy have triggered increasing interest in harnessing the power of digital location data to track, predict, and control the pandemic.

The U.S. government is already tapping bulk cell phone location data for public health surveillance purposes in the fight against COVID-19. These efforts include tracking the “presence and movement of people in certain areas of geographic interest.”¹⁰ Under new legislation, Congress appropriated “not less than \$500,000,000” for “public health data surveillance and analytics infrastructure modernization.”¹¹

Private enterprise has been quick to cooperate. Google analyzed location data from its app users’ devices to generate “COVID-19 Community Mobility Reports” for every county in the United States. These reports “chart movement trends over time by geography, across different categories of places such as retail and recreation, groceries and pharmacies, parks, transit stations, workplaces, and residential.”¹² Another much-watched visualization analyzed cell phone location data to show how the spring break population in south Florida dispersed across America. Each dot along a Florida beach during spring break marked a unique cell phone, which was followed for weeks thereafter. Spreading like delicate tendrils, this visualization of individuals’ movements illustrated “how massive the potential impact just one single beach gathering can have in spreading this virus across our nation.”¹³ These analyses by Google and others enable the government and others to discern how well the public has complied with social distancing at the individual, county, state, and national level.

The use of cell phone location data for contact tracing in a more targeted, individualized way has also garnered significant interest. Contact tracing is a traditional public health tool. The World Health Organization defines contact tracing as a monitoring process in which an infected individual identifies all other individuals with whom they may have been in contact. Those contacts are then informed, monitored, and sometimes instructed to self-isolate or quarantine.¹⁴ Contact tracing, coupled with effective isolation of relevant contacts, can “prevent further transmission of [a] virus.”¹⁵ Traditionally, contact tracing has relied on skilled workers, who interview infected individuals to learn about their activities and the people they encountered after becoming ill, and then monitor those contacts for illness. According to a recent report from the Johns Hopkins Center for Health Security, more than 100,000 contact tracers may be needed nationally to grapple with the COVID-19 pandemic.¹⁶ Massachusetts alone “plans to hire and train roughly 1,000 people to do contact tracing.”¹⁷

10 Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall St. J. (Mar. 28, 2020), <https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202>.

11 Coronavirus Aid, Relief, and Economic Security (CARES) Act, Pub. L. No. 116–136, 134 Stat. 281, 554 (2020).

12 Google, COVID-19 Community Mobility Reports, <https://www.google.com/COVID19/mobility/>.

13 Tectonix GEO (@TectonixGEO), Twitter (Mar. 24, 2020, 9:44 PM), <https://twitter.com/TectonixGEO/status/1242628347034767361>.

14 See World Health Org., Contact tracing (May 2017), <https://www.who.int/features/qa/contact-tracing/en/>.

15 *Id.*

16 See Crystal Watson et al., A National Plan to Enable Comprehensive COVID-19 Case Finding and Contact Tracing in the US 8 (Apr. 10, 2020).

17 Martha Bebinger, *Why Charlie Baker Thinks ‘Contact Tracing’ Cases May Help Mass. Slow—Or Stop—COVID-19*, WBUR (Apr. 3, 2020), <https://www.wbur.org/commonhealth/2020/04/03/contact-tracing-coronavirus-massachusetts-baker>. Other states have similar plans. See eg *What You Need to Know About New York’s ‘Mon-*

Other jurisdictions have trained their sights on cell phone data as a new, potentially more powerful, efficient, and accurate tool for contact tracing. With China, South Korea, Singapore, Israel, and others as examples, data brokers and app developers are working to bring digital contact tracing to European and American markets.¹⁸ Their pitch is enticing. In a forthcoming paper in *Science*, researchers at Oxford argue that COVID-19 spreads too quickly and asymptotically to be controllable through traditional contact tracing methods.¹⁹ To alleviate the need for long-term mass social distancing, the authors of that study argue that communities will need to deploy “instant digital contact tracing.”²⁰

Despite the public health benefits touted by proponents, it is not clear that digital contact tracing can achieve its lavish claims, nor is it evident that it can do so without imposing disproportionate privacy harms. Current technological limitations, as well as limitations in COVID-19 testing and support for quarantining identified contacts, undermine the efficacy of digital contact tracing efforts that its proponents seemingly take for granted.²¹ As for privacy, digital contact tracing efforts abroad already raise significant cause for concern. These mass surveillance programs sweep up revealing location data indiscriminately. Although they are defended on grounds of emergency and the urgent need to contend with the present health crisis, experiences in those countries already reveal the potential for abuse. Moreover, our own history amply demonstrates that surveillance powers claimed on emergency grounds frequently remain after the emergency has passed, often morphing into tools of social control targeted against disfavored individuals and groups.²²

This article assesses whether and under what circumstances the United States ought to embrace the use of epidemiological surveillance programs, including the use of cell phone location data for contact tracing purposes. Part I analyzes the constitutionality of programs like digital contact tracing, arguing that the Fourth Amendment’s protection against unreasonable searches and seizures may well regulate the use of location data for epidemiological purposes, but that the legislative and executive branches have significant latitude to develop these programs within the broad constraints of the “special needs” doctrine elaborated by the courts in parallel circumstances. Part II cautions that the absence of a firm warrant requirement for digital contact tracing should not serve as a green light for unregulated digital location tracking, whether in the form of individual or aggregate surveillance, and by means of location or proximity tracking.²³

umental’ Contact Tracing Program, NBC New York (Apr. 22, 2020), <https://www.nbcnewyork.com/news/coronavirus/what-you-need-to-know-about-new-yorks-monumental-contact-tracing-program/2385611/>.

18 Thompson, *supra* note 3. Some apps are already in use in parts of the United States and Europe. See *supra* notes 5–6 and accompanying text.

19 See Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, *Science* (Epub ahead of print Mar. 31, 2020) (forthcoming 2020), <https://science.sciencemag.org/content/early/2020/04/09/science.abb6936/tab-pdf>.

20 *Id.* at 4.

21 See *infra* notes 66–76 and accompanying text.

22 See Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Final Report Together With Additional, Supplemental, And Separate Views, Apr. 26, 1976, at 38–39, 90–92.

23 By “location tracking,” we mean the use of technologies like cell site location or GPS that monitor the movements of individual persons or devices through space. In the present context, location tracking technologies might be used to trace the movements of individuals who test positive for SARS-CoV-2 and to document potential contacts with others. By “proximity tracking,” we mean technologies like geofencing or Wi-Fi that

In light of substantial risks to privacy that a digital contact tracing program might entail, this article argues for a thoughtful, constitutionally sufficient, legislative scheme that does not indulge the hubris of emergency, assert claims of broad, unchecked power, or follow the siren's song of technovelty. Policymakers must instead ask hard questions about efficacy and the comparative advantages of location tracking versus more traditional means of controlling epidemic contagions, take seriously threats to privacy, tailor programs parsimoniously, establish clear metrics for determining success, and set plans for decommissioning surveillance programs. Should the political branches fail to perform on these duties, then the courts, as guardians of the Fourth Amendment's sacred trust, must act.

I. FOURTH AMENDMENT FRAMEWORKS

In the U.S. context, questions about protecting privacy against threats of government surveillance implicate the Fourth Amendment, which guarantees that “The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated”²⁴ Would an epidemiological surveillance program that uses cellphone location data to conduct individual contact tracing or to document and predict infection patterns using aggregate data be subject to Fourth Amendment regulation? If so, what form should those regulations take? Answering these questions requires addressing two Fourth Amendment thresholds: whether the program entails state action and whether the conduct at issue constitutes a “search” or a “seizure.”

The Fourth Amendment applies only to governments and their agents. It does not regulate the conduct of private persons or entities. Based on the surveillance programs deployed in other countries and those imagined domestically, data aggregation for contact tracing has been and will be conducted by private entities, principally cellphone service providers and technology companies with access to location data through apps installed on users' devices. This does not necessarily exhaust the Fourth Amendment inquiry, however. Under established doctrine, a private party may be subject to Fourth Amendment regulation to the extent it is acting as an agent of the state.

“Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances.”²⁵ Among the factors relevant to this inquiry are whether a government agent directed, requested, or incentivized the search, whether the private actor believed at the time that she was acting under the direction or authority of a government agent, and whether a government agent had advance notice of the search and believed that the fruits of that search would accrue to the government.

There are good reasons to believe that the cellular service providers and technology companies aggregating data for contact tracing and similar surveillance programs would

document the presence of individuals or devices in a specific area. Proximity tracking might be used to control the flow of persons in particular spaces, such as malls, grocery stores, or even cities. It might also be used to identify those who have traversed hotspots or other areas of potential contagion.

24 U.S. Const., Amend. IV.

25 *Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602, 614–615 (1989) (internal citations and quotation marks omitted).

be acting as state agents for purposes of the Fourth Amendment. Most of these entities are already routinely targets for government demands for user data—sometimes on the order of tens of thousands of requests each year. They may therefore already be acting as state agents when they collect and aggregate location data.²⁶ That case is even stronger in the narrower circumstance of epidemiological surveillance. These programs require ongoing access to historical data for baseline analysis, recent aggregate data to model population flows and contact patterns, targeted data to trace individual persons, and real-time data to monitor the activities of persons and groups. In short, these programs will entail close, ongoing public-private partnerships, which will have the effect of converting AT&T, Google, and other data collectors and aggregators into government agents for purposes of the Fourth Amendment.²⁷

To the extent doubts about the state agency requirement persist, they are probably mooted by the Supreme Court's recent decision in *Carpenter v United States*.²⁸ There, the Court held that the Fourth Amendment governs law enforcement access to historical cell site location data gathered and stored by cellphone service providers (cellphone location data, whether in the form of cell site location or GPS tracking, appears to be a centerpiece of tracing and proximity surveillance proposals because these devices are so often with their users²⁹). As the *Carpenter* Court noted, service providers collect and aggregate these data for their own business purposes.³⁰ Nevertheless, the Court held that law enforcement must secure a warrant before accessing that data in the context of a criminal investigation.³¹ The Court was decidedly mealy mouthed about what constituted the “search” in *Carpenter*, who did it, and when,³² but the circumstances contemplated by epidemiological surveillance programs are sufficiently analogous to conclude that the state agency requirement would not be an impediment to applying the Fourth Amendment, even if the precise reasons why might remain a mystery.

26 See David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 133–37 (2013).

27 There is, of course, the possibility that a purely private actor with access to individual and aggregate tracking data might attempt to engage in epidemiological surveillance completely independent of any government agent. Although we find this highly unlikely, such a truly private actor would be beyond the reach of Fourth Amendment regulation, although perhaps subject to regulation by state or federal statute. Somewhat more likely is the possibility of a private actor, such as a cellular service provider or technology company, gathering, aggregating, and making available location data, which a government agency then accesses. Again, we regard as far more likely a close, ongoing working relationship between government and private actors, but, even in this case of more limited interaction, the private actor would be a state agent for purposes of the Fourth Amendment because it *knows* that its work will be accessed and used by government agents and government agents *know* prospectively that the private actor is gathering location data to which the government will have access. See Gray & Citron, *supra* note 26, at 133–37. Moreover, the Court's recent Fourth Amendment jurisprudence indicates that the Fourth Amendment regulates government access to location information gathered by private parties. See *infra* notes 28–29 and accompanying text.

28 138 S. Ct. 2206 (2018).

29 See *Riley v. California*, 573 U.S. 373, 395 (2014) (“[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.”).

30 *Carpenter*, 138 S. Ct. at 2212.

31 *Id.* at 2221.

32 See *Id.* at 2217 (“The location information obtained from *Carpenter*'s wireless carriers was the product of a search.”); *Id.* at 2220 (“The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.”).

But does epidemiological surveillance constitute a “seizure” or a “search”? The Fourth Amendment regulates conduct that threatens the security of the people against “unreasonable searches and seizures.” Conventionally, this means that the Fourth Amendment applies only to conduct that constitutes either a “seizure” or a “search.”

“Seizures” entail material interference with property or liberty. Depending on the technology used, epidemiological surveillance programs plausibly could constitute seizures of “effects.” For example, if the government required citizens to install specific applications on their cellular phones or other electronic devices, then that interference might well amount to a seizure of effects. So, too, if government agents surreptitiously hacked devices to install tracking software.³³ In addition, if a surveillance program was aimed at using personal devices to limit users’ liberty by, say, using geofencing or other proximity tracking to enforce a physical quarantine, then that would constitute seizure of persons.³⁴

“Searches” encompass either physical intrusions into constitutionally protected areas (persons, houses, papers, or effects) for the purpose of gathering information³⁵ or intrusions upon subjectively manifested expectations of privacy that society is prepared to recognize as reasonable.³⁶ Depending on the nature of the program, epidemiological surveillance may qualify as a search under one or both of these definitions. For example, if government agents actively search data on cellular phones or other devices in order to gather location information or to access photographs and other evidence of social contacts, then their conduct might fairly be described as physically intruding upon a constitutionally protected “effect” for the purpose of gathering information.³⁷ Alternatively, if government agents access location information gathered and aggregated by third parties, such as cellular service providers or technology companies, documenting persons’ movements (or lack thereof!) over a period of time, then that would probably qualify as an intrusion upon reasonable expectations of privacy,³⁸ particularly if it revealed that they were at home.³⁹

Complications exist, to be sure. For example, what if the Centers for Disease Control (CDC) uses anonymized location data that are aggregated by a cellphone service provider or technology company and made available to researchers or business entities? Is the CDC subject to Fourth Amendment regulation if it has done nothing more than what a private party could do? In one respect, the answer is easy: “Yes, of course!” As described above, the state agency requirement highlights the fact that government agents are subject to Fourth Amendment restraints that do not bind private actors.

33 Cf. *United States v. Horton*, 863 F.3d 1041, 1046–1047 (8th Cir. 2017) (remote installation of malware on computer to gather information contents is a “search” requiring a warrant.).

34 One question that arises here is whether the attempted use of location surveillance to effect seizures of persons would trigger the Fourth Amendment. For example, what if officials pushed a text to a user’s phone notifying her that she had been exposed to the COVID-19 virus then directing her to self-quarantine for 14 days. Would that constitute a “seizure” for purposes of the Fourth Amendment? This question may be answered next Term in *Torres v Madrid*, <https://www.supremecourt.gov/docket/docketfiles/html/qp/19-00292qp.pdf>.

35 See *Florida v. Jardines*, 569 U.S. 1 (2013); *United States v. Jones*, 565 U.S. 400 (2012).

36 See *Katz v. United States*, 389 U.S. 347 (1967).

37 This kind of digital intrusion would be closely analogous to scrolling through the contents of a cellular phone, which is a “search.” See *Riley*, 573 U.S. at 401.

38 See *Carpenter*, 138 S. Ct. at 2217–20.

39 See *United States v. Karo*, 468 U.S. 705, 716–18 (1984).

In another respect, however, the answer is less clear. The Supreme Court has long allowed government agents to access through lawful means information voluntarily shared with third parties. For example, law enforcement can access information about a suspect's financial transactions through the suspect's bank or credit card servicer without worrying about the Fourth Amendment because this conduct does not intrude upon reasonable expectations of privacy.⁴⁰ In a similar vein, government agents are free to observe anyone's public movements⁴¹ or to access areas open to the public⁴² without subjecting themselves to Fourth Amendment constraints. Would either or both of these lines of cases—colloquially, the third-party and public observation doctrines—exempt epidemiological surveillance programs from Fourth Amendment scrutiny? Probably not.

In *Carpenter*, the Court held that neither the third-party nor the public observation doctrine could relieve law enforcement⁴³ from the burden of securing a warrant before accessing cell site location data that are routinely gathered and aggregated by cellphone service providers for their own business purposes.⁴⁴ The crux of the Court's reasoning was that location tracking reveals a host of intimate details about private associations and activities.⁴⁵ The Court also worried that granting law enforcement unfettered access to this kind of data would facilitate programs of broad and indiscriminate search, threatening the right of the people to be secure against threats of arbitrary state power, and conjuring the specters of general warrants and writs of assistance that haunted the minds of the founding generation.⁴⁶

Epidemiological surveillance programs robust enough to conduct individual contact tracing or to document disease progression using aggregate data will trigger these same concerns. This suggests that they, too, would be subject to some form of Fourth Amendment restraint. The fact that some of the data used might be anonymized does not change the calculus. First, as has been amply demonstrated, it is very easy to deanonymize location data.⁴⁷ That is likely to be particularly true in a world where people have been ordered to stay at home because location data will be robustly associated

40 See *United States v. Miller*, 425 U.S. 435 (1976); *California Bankers Ass'n v. Shultz*, 416 U.S. 21 (1974).

41 See *United States v. Knotts*, 460 U.S. 276 (1983).

42 See *California v. Greenwood*, 486 U.S. 35 (1988) (looking through trashcan placed at the curb for pickup is not a "search"); *Oliver v. United States*, 466 U.S. 170 (1984) (entering upon and examining "open fields" is not a search).

43 One might wonder about the application of doctrine elaborated in the context of criminal law enforcement to the quite different case of public health. It is important here to distinguish between two distinct Fourth Amendment questions: whether government action constitutes a "search," and, if so, what form of prospective restraint is necessary to guarantee the security of the people against unreasonable search. When answering the "search" question, it does not matter whether the government agent is engaged primarily in criminal law enforcement or public health. A search is a search, whether conducted by police looking for evidence of a crime or the CDC looking for traces of a contagion. By contrast, when addressing the remedy question, it matters quite a bit whether a search is conducted to advance a criminal investigation or to advance other governmental interests. See *infra* notes 51–58 and accompanying text. In addition, there are real concerns that some tracking programs justified by public health concerns may be exploited for other purposes, including law enforcement, immigration, and national security, which will require careful safeguards. See *infra* Part II.

44 *Carpenter*, 138 S. Ct. at 2220.

45 *Id.* at 2217–18.

46 *Id.* at 2213–14, 2222–23.

47 See eg, Youssf Khazbak & Guohong Cao, *Deanonymizing Mobility Tracs with Co-Location Information*, 2017 IEEE Conference on Communications and Network Security 1 (2017).

with individual residences. Second, the fact that data are anonymized may salve some of the individual privacy concerns, but it does little to resolve concerns about “arbitrary power”⁴⁸ and “permeating . . . surveillance,”⁴⁹ which threaten the Fourth Amendment right “of the people to be secure . . . against unreasonable searches and seizures.”⁵⁰

Accordingly, it is likely that epidemiological surveillance programs proposed amid the current pandemic would be subject to Fourth Amendment regulation. This does not mean that agencies like the CDC would be forbidden from using these tools or that they would be required to seek and secure a warrant based on probable cause. The Fourth Amendment allows for considerable flexibility in terms of the form of regulation it requires,⁵¹ particularly where searches are conducted to advance public policies (“special needs”) separate from criminal law enforcement.⁵²

The epidemiological surveillance programs discussed in recent months, be they individual tracking, location monitoring, or the use of aggregate data, 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. The Court has endorsed public health as a legitimate ground for special needs searches on a number of occasions⁵³ where the programs are sufficiently likely to succeed in serving a legitimate public interest⁵⁴ and stayed true to their public health goals.⁵⁵ The centerpiece of the special needs doctrine is the balancing of compelling government interests served by searches against the privacy interests of those subject to potential search. In the present context, there is no doubt that there are significant public health interests at stake. Proper interventions could well save thousands, if not hundreds of thousands, of lives while minimizing social, cultural, and economic harm.⁵⁶ These weighty public interests cannot sign a constitutional blank check, however. The Fourth Amendment still requires some form of constitutionally sufficient prospective constraint on searches and the discretionary authority of agents to conduct searches.

48 *Carpenter*, 138 S. Ct. at 2214 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

49 *Id.* (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

50 David Gray, *The Fourth Amendment in an Age of Surveillance* 146–56 (2017) (explaining collective dimensions of Fourth Amendment rights).

51 David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. Rev. 425, 462–83 (2016).

52 *New Jersey v. T. L. O.*, 469 U.S. 325, 351 (1985).

53 See e.g. *Bd. of Educ. of Indep. Sch. Dist. of Pottawatomie Cty. v. Earls*, 536 U.S. 822 (2002) (drug testing of high school students engaged in extracurricular activities); *Vernonia Sch. Dist. 47 J v. Acton*, 515 U.S. 646 (1995) (drug testing of high school athletes).

54 But see *Chandler v. Miller*, 520 U.S. 305, 320–21 (1997) (declining to approve a mandatory drug testing regime for Georgia politicians, in part, because the regime was merely “symbolic” and unlikely to achieve its purported goals).

55 But see *Ferguson v. City of Charleston*, 532 U.S. 67, 79–80 (2001) (recognizing that public health can provide grounds for justifying special needs searches, but declining to endorse on special needs grounds a program whose real purpose was to advance ordinary law enforcement goals).

56 This seems to be congressional motivation for funding epidemiological surveillance through the CARES Act. See *supra* note 11 and accompanying text.

Special needs searches generally do not require a warrant.⁵⁷ In these noncriminal contexts, the Court has endorsed a variety of regulatory approaches that serve legitimate public policy interests while still guaranteeing the right of the people to be secure from threats of unreasonable searches and seizures. Executive agencies and legislatures play a key role in this context. Courts tend to grant the political branches broad latitude to develop and deploy administrative and programmatic structures regulating the use of searches that serve goals such as public health as long as they are narrowly tailored, likely to succeed, strike a reasonable balance between privacy interests and public policy goals, and limit the discretion of government agents conducting searches.⁵⁸ The next part details a framework that policymakers can apply to meet these constitutional demands when deploying and using epidemiological surveillance tools such as contact tracing.

II. LEGISLATING DIGITAL CONTACT TRACING IN THE SHADOW OF THE FOURTH AMENDMENT

The COVID-19 pandemic poses an emergency for public health. Faced with such emergencies, executive agents are wont to assert broad discretionary powers. As the Canadian Freeholder observed in 1779, they are

fond of doctrines of reason of state, and state necessity, and the impossibility of providing for great emergencies and extraordinary cases, without a discretionary power in the crown to proceed sometimes by uncommon methods not agreeable to the known forms of law.⁵⁹

The Fourth Amendment guards against these threats, “curb[ing] the exercise of discretionary authority” to search and seize.⁶⁰ To deploy and use epidemiological surveillance tools will therefore require more than executive fiat. What the Fourth Amendment demands is a clear and deliberative process, weighing the genuine benefits and costs of programs likely to engage in invasive and potentially mass surveillance. This process—which should involve both legislative and agency actors—must identify prospective remedial measures sufficient to safeguard the right of people to be secure

57 See *Michigan v. Sitz*, 496 U.S. 444 (1990) (roadblock checkpoints to screen for drunk drivers are reasonable in light of the goal of protecting public safety); *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656 (1989) (the fact that border control agents carry firearms may provide reasonable public safety grounds for drug testing); *Skinner v. Ry. Labor Execs. Ass’n*, 489 U.S. 602 (1989) (drug testing of railroad workers involved in accidents is reasonable in light of interest in protecting public safety). *Cf. Ferguson*, 532 U.S. at 80 (municipal program requiring drug testing pregnant women on public health grounds fell outside the special needs doctrine because positive results were reported to law enforcement).

58 See *eg Earls*, 536 U.S. 822 at 844–46 (Ginsburg, J., dissenting) (expressing concern that subjecting all high school students engaged in extracurricular activities to drug testing casts too broad a net); *Indianapolis v. Edmond*, 531 U.S. 32 (2000) (declining to endorse drug interdiction roadblocks due, in part, to the fact that driving is a relatively common activity and interdicting drugs is not closely tied to automobile safety); *Chandler*, 520 U.S. at 320–21 (declining to endorse a drug-testing regime aimed at politicians, in part, because the program was unlikely to succeed in detecting actual drug use).

59 2 Frances Maseres, *The Canadian Freeholder: In Three Dialogues Between an Englishman and a Frenchman, Settled in Canada 243–44* (London, B. White 1779) (commenting on *Wilkes v. Wood* (1763) 98 Eng. Rep. 489 (KB)).

60 See Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 556 (1999) (“[T]he larger purpose for which the Framers adopted the [Fourth Amendment] was to curb the exercise of discretionary authority by officers.”).

against unreasonable searches and seizures while reasonably accommodating legitimate public health goals.

In other work, one of us has elaborated a constitutionally informed framework policymakers can apply when designing data surveillance programs.⁶¹ This framework challenges the political branches to engage critical questions about need, efficacy, parsimony, and discretion before deploying these kinds of surveillance tools. It also provides a guide for courts to evaluate the constitutional sufficiency of the regulatory structures erected around these kinds of surveillance programs.⁶² Below, we explain how that framework might guide the development and deployment of public health surveillance programs like digital contact tracing, location monitoring, and data aggregation and analysis.

Predeployment review. Before a digital public health surveillance program is deployed, proponents must publicly and transparently identify the goals of the program and establish a reasonable, scientifically grounded fit between those goals, the methods to be used, and the data to be gathered.⁶³ In particular, proponents must clearly articulate why digital methods outperform traditional alternatives in order to justify additional intrusions on privacy.

Contact tracing is a well-established component of ordinary public health measures. Historically, contact tracing has utilized skilled workers to conduct interviews, contact potentially infected individuals, and counsel and diagnose those individuals throughout a monitoring or quarantine period. But there is emerging evidence that digital contact tracing may have substantial benefits over traditional methods of interview and direct contact, given the unique attributes of COVID-19. Recent modelling data comparing traditional and digital contact tracing methods have indicated that COVID-19 spreads too quickly and often asymptotically to be controllable through traditional contact tracing methods.⁶⁴ According to some researchers, “instant digital contact tracing” will be necessary to transition out of mass social distancing.⁶⁵

Digital contact tracing cannot hope to achieve its promised benefits, however, without necessary precursors and responses. For instance, although the United States has expanded COVID-19 testing, its per capita level of testing still lags many countries, including several at the forefront of digital contact tracing.⁶⁶ Effective identification of infected individuals is a pre-requisite to effective contact tracing efforts. Absent testing capacity and procedures robust enough to give confidence that infected individuals are

61 See Gray, *supra* note 50, at 267.

62 See Lindsay F. Wiley & Steve Vladeck, *Coronavirus, Civil Liberties, and the Courts: The Case Against ‘Suspending’ Judicial Review*, Harv. L. Rev. F. (forthcoming 2020), <https://blog.harvardlawreview.org/covid-19-reinforce-the-argument-for-regular-judicial-review-not-suspension-of-civil-liberties-in-times-of-crisis/>. As Wiley & Vladeck make clear, courts must not abdicate their role in superintending and ensuring compliance with constitutional protections, even in the face of a pandemic.

63 *Id.* at 267.

64 See Ferretti et al., *supra* note 19.

65 *Id.* at 4.

66 See Worldometer, COVID-19 Coronavirus Pandemic (Apr. 30, 2020, 04:41 GMT), <https://www.worldometers.info/coronavirus/#countries> (reporting that the United States has tested 18,549 per one million population, with countries including Singapore, Hong Kong, and Israel, as well as Canada, Spain, Ireland, Italy, and Germany, among others, reporting higher testing rates per one million population).

likely be identified rapidly, collecting and storing mass location data are likely to impose significant privacy harms without corresponding public health benefits.⁶⁷

Previous infectious disease mitigation efforts reinforce the need to prioritize traditional processes before resorting to technologically enhanced surveillance. In 2014, a West African outbreak of Ebola eventually made its way to the United States.⁶⁸ The first case of U.S. Ebola was Thomas Eric Duncan, who had contact with an Ebola patient in Liberia 4 days before traveling to the United States. Although Duncan should have been screened before departing Liberia, that screening did not occur. Moreover, when Duncan presented with symptoms at a Texas emergency room, “somehow doctors were unaware that he had recently traveled from one of the West Africa countries where Ebola [was] spreading rapidly. He was sent home, highly infectious.”⁶⁹ Duncan eventually succumbed to Ebola, but not before infecting two of his caregivers. As one commentator concluded, “Ebola is a tragic reminder of the power of the process.”⁷⁰ Efforts to use aggregate digital data in other public health surveillance efforts have reached similar conclusions.⁷¹

Reliable processes to identify infected individuals must be followed by efficient procedures to inform and monitor any contacts who may have been exposed. In the case of COVID-19, current proposals for digital contact tracing largely appear to take for granted that identified contacts will immediately and reliably self-isolate for the 2-week incubation period of a possible COVID-19 infection. The Oxford research team that advocates “instant digital contact tracing” plainly states that it modelled the impact of “tracing the contacts of symptomatic cases *and quarantining them*.”⁷² Their model defines its success rate as “the fraction of all contacts traced, assuming perfectly successful quarantine upon tracing, or the degree to which infectiousness of contacts is reduced assuming all of them are traced.”⁷³ That is a generous assumption with no demonstrated grounding in reality.

Our recent experience with social distancing suggests that many people will continue to congregate, whether by choice or necessity, despite prompts to maintain social distance. Pictures abound of crowded subways, public markets, houses of worship, beaches, and parks across the country.⁷⁴ Workers without paid sick leave—let alone

67 To be sure, contact tracing may hold value even absent a perfectly robust testing regime. But in light of the deep and broad privacy risks that digital contact tracing programs may impose, in particular, the robustness of the testing regime—and other less high-tech matters—substantially affects the balance of benefits and harms at the core of the special needs analysis.

68 CDC, 2014–2016 Ebola Outbreak in West Africa (Mar. 8, 2019), <https://www.cdc.gov/vhf/ebola/histories/2014-2016-outbreak/index.html>.

69 Jeanne Roué-Taylor, *Ebola Shows It Is Process—Not Technology—That Will Protect Us*, *Wired* (Oct. 2014), <https://www.wired.com/insights/2014/10/ebola-process-not-technology/>.

70 *Id.*

71 See David Lazer & Ryan Kennedy, *What We Can Learn From the Epic Failure of Google Flu Trends*, *Wired* (Oct. 1, 2015), <https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/> (describing how Google Flu, which aimed to predict flu prevalence based on aggregate location-tracked search queries, “failed spectacularly”).

72 Ferretti et al., *supra* note 19, at 4 (emphasis added).

73 *Id.*

74 See eg Minyonne Burke, *Crowds Gathered at National Mall to Watch Blue Angels, Thunderbirds Flyover*, *NBC News* (May 2, 2020), <https://www.nbcnews.com/news/us-news/crowds-gathered-national-mall-watch-blue-angels-thunderbirds-flyover-n1198706>; *Coronavirus News: Social Distancing Is Not Happening on the NYC Subway*, *ABC7* (Apr. 1, 2020), <https://abc7ny.com/overcrowded-subway-train-nyc-social-distancing->

paid leave for possible, but unconfirmed, infection—may simply be unable to afford to self-isolate when prompted by public health orders, even if they are otherwise inclined to obey. From a purely practical perspective, then, models grounded in assumptions about compliance with self-isolation instructions offer little in terms of evidence that digital tracing methods will be superior enough to traditional methods to justify the radical costs to privacy attendant to mass surveillance.

Moreover, digital contact tracing may cast so wide and impersonal a net that it will be less effective than traditional means in generating compliance. Depending on the precision of the location data, prompts to self-isolate may become overbroad and routine, which will further reduce compliance. Social distancing recommendations emphasize 6 feet of distance between people to minimize infection. This suggests that ideal contact tracing would limit its scope to individuals who were within 6 feet of an infected person. But cell tower and GPS data typically have margins of error of more than 6 feet. GPS data, which is more precise than cell tower location data, is usually accurate only to within 16 feet, with even poorer performance in crowded urban areas.⁷⁵ Bluetooth tracking may be more precise, but it is also overinclusive, likely registering contacts between devices despite the presence of walls, car doors, or even whole floors in a building.⁷⁶

At least for now, these tools are likely to direct into isolation many people who were never actually at risk. Over time, overbroad notifications will fail to prompt appropriate self-isolation even among individuals who are genuinely at risk—the epidemiological equivalent of crying “wolf!” Other difficulties may arise as well, from false or malicious designations of an individual as infected when they are not, to insufficient participation in voluntary programs. Traditional contact tracing, though perhaps a bit slower, may still prove to be more precise, accurate, robust, reliable, and visceral, and therefore may be more effective in generating actual compliance.

In sum, digital contact tracing is unlikely at present to yield its promised benefits due to low testing rates, low compliance rates, and technological limitations. Before requesting or requiring individuals to sacrifice their locational and associational privacy, policymakers must ensure that the screening, testing, and isolating of affected individuals can be done at comparable scale. Similarly, before aggregate location data are gathered or analyzed, policymakers should ensure that there is sound evidence of efficacy and accuracy of such tools, beyond what traditional public health surveillance methods can generate. Absent such assurances, Americans would be surrendering substantial privacy without concrete gains in public health, safety, or liberty.⁷⁷

coronavirus/6068366/; Nick Boykin & Sarah Konsmo, *DC Mayor Closes Wharf Fish Markets after Patrons Fail to Follow Social Distancing Guidelines*, WUSA9 (Apr. 4, 2020), <https://www.wusa9.com/article/news/health/coronavirus/wharf-fish-market-packed-on-a-saturday-social-distancing-not-being-practiced/65-334f226a-e56a-45d9-82f3-e6ad129a60fe>.

75 See *Carpenter*, 138 S. Ct. at 2219 (touting improved cell tower triangulation methods giving location precision to within 50 m); GPS.Gov, GPS Accuracy (Dec. 5, 2017), <https://www.gps.gov/systems/gps/performance/accuracy/> (“GPS-enabled smartphones are typically accurate to within a 4.9 m (16 feet) radius under open sky”). Nonetheless, the majority of existing digital contact tracing apps appear to rely on GPS data. See Woodhams, *supra* note 6 (observing that 57% of current apps use GPS data).

76 Tony Romm et al., *Apple, Google Debut Major Effort to Help People Track if They've Come into Contact with Coronavirus*, Wash. Post (Apr. 10, 2020), <https://www.washingtonpost.com/technology/2020/04/10/apple-google-tracking-coronavirus/>.

77 The American Civil Liberties Union has sounded similar concerns about efficacy in a recent white paper on technology-assisted contact tracing. See Daniel Kahn Gillmor, *Principles for Technology-Assisted Contact-*

Even if an epidemiological surveillance program can establish efficacy, that does not end the Fourth Amendment inquiry. Given the substantial privacy interests at stake, legislators and app developers must take care at all stages of design, deployment, and use to mitigate against privacy harms, beginning with data gathering. Indeed, these later stages—and the need to continue to probe issues of efficacy—will take on increased importance if app developers or policymakers charge ahead before pre-deployment review is completed.⁷⁸

Data gathering and aggregation. Epidemiological surveillance programs such as digital contact tracing should gather the minimum amount and types of data reasonably necessary to facilitate their public health goals. Although GPS data are seemingly ubiquitous, it casts too wide a net and thus exposes a larger population's location data in response to every query. Bluetooth data, by contrast, may be able to register proximity between devices more precisely, alongside or instead of logging location directly.⁷⁹ Utilizing proximity data rather than location data could minimize the intrusiveness of the data gathered because these data would reveal that two devices were in proximity but not where. Limiting the timeframe covered by location or proximity data would minimize the scope of information revealed about a person's movements, habits, and intimate associations.⁸⁰

Policymakers should also mandate information siloing to the extent possible. Information silos “establish or maintain separation between databases, thereby setting limits on the breadth and generality achieved by aggregation.”⁸¹ Where possible, data should be stored locally on a device or with the entity that initially gathered it. This limits the government's ability to make secondary uses of sensitive data. Congress used this approach in the 2015 USA Freedom Act, which amended the National Security Agency's telephony metadata program so that metadata would remain with telephone companies until queried, rather than being turned over to the National Security Agency in bulk.⁸²

Tracing, Am. Civil Liberties Union 2 (Apr. 16, 2020), <https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing>.

78 See *eg supra* notes 5–6 and accompanying text (charting the proliferation of digital contact tracing apps, including in some U.S. states).

79 *Id.*

80 In addition to satisfying the Fourth Amendment, data gathering, aggregation, and other features of a digital contact tracing effort must also comply with existing statutory privacy protections. For instance, the California Consumer Privacy Act provides California residents with, among other rights, the right to know what information certain businesses have collected about them, the right to request deletion of that data, and the right to opt out of the sale of that data to others. See Cal. Civ. Code § 1798.100–1798.199. Similar statutory constraints exist under Europe's General Data Protection Regulation (“GDPR”). See Regulation 2016/679 of the European Parliament and of the Council of 27 Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1; European Data Protection Bd., Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak (Apr. 21, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (providing guidance on harmonizing digital contact tracing efforts in Europe with GDPR and other European privacy laws). Guidance under these statutory frameworks may, in significant respects, mirror the approach advocated in this Article, including preferring proximity data and requiring limited and exclusive purposes for which data may be used. See *Id.* at 7 (outlining “general legal analysis” for “contact tracing applications”).

81 Gray, *supra* note 50, at 269.

82 *Id.* at 270.

Similarly, keeping digital location trails out of government hands would help mitigate the privacy threats of contact tracing programs. Thus far, digital contact tracing efforts have relied on centralized administration by governments, putting mass location data in government hands. This includes an app for digital contact tracing that the European Union will soon roll out, beginning in Germany.⁸³ But there may be alternatives that decentralize data storage, limiting threats of mass surveillance. For instance, a team at University College London designed a framework that “focuses on decentralization and . . . stops any personal data leaving a device.”⁸⁴ If accurate and effective, a decentralized approach would help mitigate privacy harms while preserving important public health goals.

Data storage. The privacy harms of digital location tracking are exacerbated the longer tracking lasts and the longer data remain available to government agents.⁸⁵ The Supreme Court has recognized that the time-machine nature of digital location tracking is inconsistent with “a central aim of the Framers . . . to place obstacles in the way of a too permeating police surveillance.”⁸⁶ Strict durational limits on data collection, storage, and destruction are vital to minimize threats to privacy posed by epidemiological surveillance programs.

For example, current public health practice recommends a 2-week quarantine or active monitoring period for individuals potentially infected with the COVID-19 virus.⁸⁷ A similar durational limit would be appropriate for location data utilized for digital contact tracing. Only contacts within that 14-day period are likely to be at risk of infection, with more temporally distant contacts having interacted with the infected person before they were infected or contagious. It therefore seems that location data should be collected and retained only for 2 weeks at a time, after which it should be destroyed. Insofar as there may be good reasons to extend this window, the point remains that it is important to set limits on how much data are retained and for how long.

Data access, analysis, and use. Access to the data gathered, aggregated, and stored as part of an epidemiological surveillance program—and authority to query that data—should be strictly limited to those whose access is essential for the program to function. These data should not be available to people, groups, or algorithms for purposes unrelated to digital contact tracing and certainly should not be open source. The reason is straightforward: Mission creep imperils the success and constitutional soundness of such a program as does the risk of abuse.

83 See Zak Doffman, *COVID-19's New Reality—These Smartphone Apps Track Infected People Nearby*, *Forbes* (Apr. 7, 2020), <https://www.forbes.com/sites/zakdoffman/2020/04/07/COVID-19s-new-normal-yes-you-r-phone-will-track-infected-people-nearby/#790dd4b17f0d>.

84 *Id.*

85 Cf. *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2178 (2016) (explaining that taking blood samples and preserving them for extended periods of time “may result in anxiety for the person tested” due to the potential that these samples may be subject to tests revealing personal information about donors).

86 *Carpenter*, 138 S. Ct. at 2214, 2218 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

87 See Stephen A. Lauer et al., *The Incubation Period of Coronavirus Disease 2019 (COVID-19) From Publicly Reported Confirmed Cases: Estimation and Application*, *Annals of Internal Med.* (Epub ahead of print Mar. 10, 2020) (forthcoming 2020) (reporting a median incubation period of 5.1 days, with 99% of cases presenting symptoms within 14 days).

For instance, mass digital location data would surely aid the Department of Justice in investigating and prosecuting crimes or the Department of Homeland Security in tracking and arresting undocumented immigrants in the United States. But these uses would plainly diverge from the purposes undergirding this digital location data program. So, too, would a functionary's use of the data to trace a former spouse's movement and associations. Just as data should be siloed to prevent its misuse, access and authority to query these data should be zealously guarded, privileging public health efforts and excluding law enforcement or other efforts. Absent such segmentation, the Supreme Court's recent epistle on digital location privacy in *Carpenter* would be meaningless.

Similarly, even within the public health arena, the use of this mass surveillance data must be strictly limited to its intended purpose. For instance, while digital location data might be accessible to public health officials engaged in contact tracing efforts, it would be inappropriate for those data to be accessible to government officials charged with enforcing general social distancing orders.⁸⁸ This constitutes a separate purpose requiring independent justification. Moreover, if decentralization of data is possible, then direct access by any government entity might well be unnecessary and therefore inappropriate.

The program must end. A well-designed and well-justified epidemiological surveillance program designed to combat COVID-19 must be coupled with strict sunset provisions. The War on Terror, launched in the wake of the 9/11 attacks, is instructive in the way that demands for emergency authority can act as one-way ratchets, effecting permanent expansions of surveillance powers, and how crises can metastasize, developing into perpetual claims of emergency. It is telling that, in the midst of the current crisis, Congress once again granted a reprieve to the National Security Agency's troubled Section 215 program, which originated the bulk collection of telephonic metadata.⁸⁹ Once a tool like contact tracing is operational, it will be tempting for public health officials to utilize this tool to combat other infectious diseases. Seasonal influenza, after all, sickens millions and kills thousands each year.⁹⁰ The ability to more easily track and trace the flu would surely aid public health efforts. Yet this, too, would constitute unjustified mission creep.

Recursive review. Finally, audit procedures should be required to ensure accountability after the fact. Audit trails or other documentation should enable review of who gains access to sensitive location data, on what authority, and for what queries. In addition, program managers should conduct regular reviews to determine whether the promises of a program match its reality.

88 But see Gian Volpicelli, *The NHS Coronavirus App Could Track How Long You Spend Outside*, Wired (Apr. 7, 2020), <https://www.wired.co.uk/article/nhs-coronavirus-tracking-app>.

89 See India McKinney, *Enough is Enough—Let it Expire*, Elec. Frontier Found. (Mar. 18, 2020), <https://www.eff.org/Enough-is-enough-let-215-expire>. Congress has also repeatedly extended other controversial surveillance programs, despite apparent sunset or reauthorization provisions, including Section 702 of the FISA Amendments Act of 2008. See *Decoding 702: What is Section 702?*, Elec. Frontier Found., <https://www.eff.org/702-spying> (last visited Apr. 30, 2020) (observing that “[c]urrently, Congress has to renew Section 702 every few years. It was last renewed in 2018 and is set to expire at the end of 2023.”).

90 See CDC, *Disease Burden of Influenza* (Jan. 10, 2020), <https://www.cdc.gov/flu/about/burden/index.html>.

CONCLUSION

Epidemiological surveillance programs such as digital contact tracing have been touted as a silver bullet that will free the American public from the strictures of social distancing, enabling a return to school, work, and socializing. But these tools also tread on established expectations of privacy while presenting real threats of persistent mass surveillance. In sorting through these promises and challenges, the Fourth Amendment will have a critical role to play. Like all provisions of in the Bill of Rights, it imposes limits on what the political branches can do, no matter how popular or seemingly necessary in “providing for great emergencies and extraordinary cases.”⁹¹ In particular, the Fourth Amendment will require that epidemiological surveillance programs demonstrate sufficient potential to serve compelling public health goals.

There are good reasons to be skeptical. Unless and until more mundane aspects of contact tracing are operating efficiently—including availability of testing and practical support for appropriate self-isolation by contacts—there is little reason to think that there is enough promise to justify the dramatic expansions in government power and significant costs to personal privacy.

Even if there is good reason to believe in the public health promise of these programs, the Fourth Amendment requires more than blind faith in the judgment of government officials. The Fourth Amendment is genetically skeptical of granting broad, unfettered discretion for state agents to conduct searches and seizures.⁹² To meet Fourth Amendment demands, epidemiological surveillance programs, whether directed at digital contact tracing, location monitoring, or data aggregation and analysis, must be the products of rigorous deliberative processes, weighing the genuine benefits and costs. Robust prospective remedial measures should be put in place to secure privacy and liberty, including limitations on data gathering, aggregation, storage, access, analysis, and use. In addition, programs should be subject to constant review and sunset provisions. Only by adopting these kinds of procedural and substantive safeguards can we hope to achieve legitimate public health goals as we face COVID-19 while also protecting our sacred constitutional trust.

91 2 Maseres, *supra* note 59, at 243–44.

92 See *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).