0091-4169/21/11104-0909
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 111, No. 4
 Printed in U.S.A.

CRIMINOLOGY

CONSTITUTIONAL PANDEMIC SURVEILLANCE

MATTHEW B. KUGLER[*] & MARIANA OLIVER[**]

How do people view governmental pandemic surveillance? And how can their views inform courts considering the constitutionality of digital monitoring programs aimed at containing the spread of a highly contagious diseases? We measure the perceived intrusiveness of pandemic surveillance through two nationally representative surveys of Americans. Our results show that even at the height of a pandemic people find surveillance for public health to be more intrusive than surveillance for traditional law enforcement purposes. To account for these strong privacy concerns, we propose safeguards that we believe would make cell phone location tracking and other similar digital monitoring regimes constitutionally reasonable.

* Matthew B. Kugler is an Associate Professor of Law at Northwestern Pritzker School of Law. The authors thank Anne Boustead, Zachary Clopton, David Hoffman, Tonja Jacobi, Katherine Litvak, John McGinnis, Janice Nadler, Martin Redish, Meredith Roundtree, David Schwartz, Nadav Shoked, and Matthew Spitzer for their helpful comments on earlier drafts of this manuscripts, and Ann Herman and Joel Mackler for research assistance.

** Mariana Oliver is a JD/PhD candidate in Sociology at Northwestern University.

INTRODUCTION

As the COVID-19 pandemic hit the United States in early 2020, Americans were inundated with media reports about novel forms of public health surveillance. Apple and Google formed a partnership to create a smartphone contact tracing application.[1] News sites began to create "mobility trend" reports that showed how much smartphone users were moving about, week to week, in different states and cities.[2] And media organizations produced sharable visuals showing how the cell phones of those gathered in particular locations at particular times, such as Florida beachgoers on a busy weekend, then dispersed across the nation.[3]

Alongside their infotainment value, these displays also showed the potential power of digital pandemic monitoring. Want to enforce a 14-day quarantine period for those entering your state?[4] You could troll social media

---

[1] Chris Ip, *The Importance of Apple and Google's Rare Collaboration on Contact Tracing*, ENGADGET (Apr. 13, 2020), https://www.engadget.com/apple-google-contact-tracing-explainer-170056298.html [https://perma.cc/8U7Q-PGE7].

[2] Justine Coleman, *Apple Now Sharing Mobility Data from Apple Maps to Help Public Health Authorities*, HILL (Apr. 14, 2020, 3:28 PM), https://thehill.com/policy/technology/technology/492763-apple-now-sharing-mobility-data-from-apple-maps-to-help-public [https://perma.cc/4QM3-REHV].

[3] Jason Murdock, *Mobile Phone Location Data of Florida Beachgoers During Spring Break Tracked to Show Potential Coronavirus Spread*, NEWSWEEK (Mar. 27, 2020, 11:11 AM), https://www.newsweek.com/x-mode-tectonix-coronavirus-heat-map-tracking-mobile-data-covid-19-spring-break-1494663 [https://perma.cc/M8MY-FQ5P].

[4] *See generally* Katherine Rosenberg-Douglas, *Chicago's Travel Quarantine Order Adds 2 States and D.C. to Orange List, Knocks 1 Off Red List. Here's What You Need to Know to Avoid a Large Fine.*, CHI. TRIB. (Nov. 17, 2020), https://www.chicagotribune.com/coronavirus/ct-cb-coronavirus-chicago-self-quarantine-rules-to-know-20200729-rzt3x7jj5fbsxi2ewq4oxvgs5i-story.html [https://perma.cc/Z3VJ-XE32] (stating that anyone who spent more than a day in any of 26 states should quarantine upon their return or face fines of up to $500 per day); Ted Armus, *They Were Arrested and Jailed for Breaking a Quarantine Order. They're Not*

for vacation photos, or you could monitor whose cell phones entered the state and then evaluate how much those phones moved once they arrived. You could also use this data for contact tracing by flagging phones that have been near those of a person who was discovered to be infected.[5]

This kind of surveillance was not uncommon overseas in the spring of 2020. Many other countries were using cell phone location data—sometimes GPS, sometimes Bluetooth—to track the movements of infected people and enforce quarantine orders.[6] Countries including China, Taiwan, Israel, and South Korea also used this data for contact tracing.[7] Though digital tracing has been used in the past, the scale of these efforts dwarfed anything previously seen.[8]

These overseas developments prompted considerable discussion about whether the U.S. Constitution permits mass digital pandemic surveillance, particularly through innovative use of cell phone location data.[9] Though the Fourth Amendment has been most discussed in the context of criminal investigations, the Amendment's protection against "unreasonable searches and seizures" applies to all government information gathering programs, not just criminal ones.[10] Both a public health contact tracing program and a law enforcement-directed quarantine enforcement program would have to comply with it.

---

the First., WASH. POST (July 31, 2020, 6:02 AM), https://www.washingtonpost.com/nation/2020/07/31/arrest-breaking-quarantine-covid-florida/ [https://perma.cc/2C98-MFR6] (review-ing examples of criminal quarantine enforcement).

[5] Chas Kissick, Elliot Setzer & Jacob Schulz, *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/RC9U-KNV5].

[6] Isobel Asher Hamilton, *Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, and It's Part of a Massive Increase in Global Surveillance*, BUS. INSIDER (Apr. 14, 2020, 10:30 AM), https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3 [https://perma.cc/RHM2-6T3F].

[7] Kim Lyons, *Governments Around the World Are Increasingly Using Location Data to Manage the Coronavirus*, VERGE (Mar. 23, 2020, 2:21 PM), https://www.theverge.com/2020/3/23/21190700/eu-mobile-carriers-customer-data-coronavirus-south-korea-taiwan-privacy [https://perma.cc/3YBX-ZQEP].

[8] *See infra* notes 169, 182.

[9] *See, e.g.*, Alan Z. Rozenshtein, *Disease Surveillance and the Fourth Amendment*, LAWFARE (Apr. 7, 2020, 1:54 PM), https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment [https://perma.cc/2NSH-4VRY] (describing Fourth Amendment issues); Elliot Setzer, *Contact-Tracing Apps in the United States*, LAWFARE (May 6, 2020, 4:08 PM), https://www.lawfareblog.com/contact-tracing-apps-united-states [https://perma.cc/59NP-99XN] (reviewing the landscape of apps).

[10] *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

As we explore in Part I, Fourth Amendment doctrine is unfortunately poorly developed outside the context of law enforcement investigations. When the government is engaged in information collection for "special needs" beyond "general crime control," the constitutionality of the program is assessed using a relatively free-form reasonableness balancing test.[11] This analysis could easily be criticized as ill-defined, with each "special need" search domain being so individuated as to lack common principles.[12] As special needs cases span many different topics—from border searches to public schooling to government personnel management—there is indeed much variation.[13] Nevertheless, the cases continually emphasize some common factors: the distinctiveness of the person or relationship giving rise to the search, the intrusiveness of the search, the potential for arbitrary enforcement to lead to abuse, and the strength of the government's interest in conducting the search.

Because intrusiveness is a central part of the special needs analysis, in Part II we seek to quantify the intrusiveness of pandemic surveillance relative to the better understood category of law enforcement surveillance. This follows a tradition of Fourth Amendment scholarship that uses public opinion data to better understand privacy values.[14] Consistent with this scholarly approach, we conducted two studies with a total of almost 2,400 participants in the spring and summer of 2020—the height of the pandemic in the U.S.

The data from these studies show that people view surveillance aimed at controlling a health pandemic as even more intrusive than surveillance aimed at facilitating the traditional activities of law enforcement. For example, surveillance conducted by public health agents for contact tracing and by police to enforce a stay-at-home order are both considered more intrusive than traditional law enforcement monitoring. People felt this way during the height of the first wave of the pandemic in early April 2020, and they still felt this way after the United States had experienced over 100,000 deaths attributable to COVID-19 in June 2020. This surprising result—doubly shocking given the context of thousands of COVID deaths per day and an almost universal lockdown during the first round of data collection—should be taken seriously by public health officials and political leaders aiming to assess the privacy cost of mass pandemic surveillance.

---

[11] *See infra* Section I.B.

[12] *See, e.g.*, Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1150–52 (1998) (arguing that Fourth Amendment law is full of conceptually "local" issues and that attempts to extract a general theory of the Fourth Amendment are doomed to frustration).

[13] *See infra* notes 66–91.

[14] *See infra* notes 103–111.

In Part III we apply the results from these surveys to a Fourth Amendment reasonableness analysis to assess what kind of pandemic surveillance would be constitutionally acceptable. Though some technologies that are useful for pandemic surveillance fall outside of traditional Fourth Amendment protection, the most useful—cell phone location data—is generally covered. Because digital contact tracing by public health authorities likely falls within the special needs category, courts must balance the intrusiveness of the search versus the public benefit. Given the public's perception of the extreme intrusiveness of the searches, this article suggests that tight controls and safeguards are needed to make digital contact tracing reasonable. Absent those controls, such surveillance likely violates the Fourth Amendment and the constitutional right to information privacy. This article therefore proposes guidelines that would minimize the constitutional problems raised by pandemic surveillance, drawing inspiration from the regime for prescription drug tracking that the Supreme Court approved in *Whalen v. Roe*.[15]

I. FOURTH AMENDMENT SEARCHES IN THE PANDEMIC CONTEXT

The Fourth Amendment requires that government searches be reasonable.[16] This means that when engaging in Fourth Amendment analysis, one first asks whether an act of government information collection constitutes a "search" and then, second, whether the search is a reasonable one.[17]

Currently, Fourth Amendment law is deeply unsettled about whether precisely the kinds of surveillance most at issue in the COVID context constitute searches.[18] Specifically, the kinds of pandemic surveillance that have been considered include cell phone location data, surveillance video footage from cameras in public places, video from drones, facial recognition technology, and credit and utility records.[19] Entire papers have been written

---

[15] 429 U.S. 589, 600 (1977).

[16] U.S. CONST. amend. IV (guaranteeing the people's right to be free from "unreasonable searches and seizures").

[17] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (if a search, must assess reasonableness); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (no warrant required if not a search).

[18] *See infra* Section I.A.

[19] *See* Deborah Brown & Amos Toh, *Technology Is Enabling Surveillance, Inequality During the Pandemic*, HUM. RTS. WATCH (Mar. 4, 2021, 12:01 AM), https://www.hrw.org/news/2021/03/04/technology-enabling-surveillance-inequality-during-pandemic [https://perma.cc/GNQ5-TZ3L]; Seth Colaner, *The Technologies the World Is Using to Track Coronavirus — and People*, VENTUREBEAT (May 18, 2020, 9:16 AM), https://venturebeat.com/2020/05/18/the-technologies-the-world-is-using-to-track-coronavirus-and-people/

about whether using some of those sources of information would normally qualify as a "search" under normal conditions.[20] In Section I.A, this article will briefly review the extent of that uncertainty. In Section I.B, this article will examine the kinds of law enforcement searches that count as special needs searches. In Section I.C this article will turn to the role of intrusiveness in evaluating the reasonableness of non-law enforcement searches.

A. GOVERNMENT INFORMATION GATHERING AND THE DIGITAL REVOLUTION

Five of the seven scenarios used in Part II's study of pandemic-related attitudes are fundamentally about companies' business records.[21] These include: cell phone location information, credit card information, and utility information. Of these, cell phone location information is by far the most important and most discussed in the pandemic context; it can directly track the movements of infected people and their contacts.

Under the third-party doctrine, the Fourth Amendment has historically granted no protection for this type of consumer business record.[22] The government's acquisition of this information is not considered a "search" for Fourth Amendment purposes and therefore courts do not even reach the question of whether the acquisition is reasonable.[23] Essentially, the information is treated as non-private. The basic logic is that people have voluntarily chosen to share their customer information with the third-party company, and therefore have abandoned their privacy interest in it.[24]

The shape of Fourth Amendment law has shifted substantially over the last 10 years, however. In *United States v. Jones*,[25] two concurring opinions

---

[https://perma.cc/9LT7-W2PM]; Dave Gershgorn, *We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World*, ONEZERO (Apr. 9, 2020), https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 [https://perma.cc/S9WP-8RD7].

[20] *See, e.g.*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021); Matthew B. Kugler & Meredith Hurley, *Protecting Energy Privacy Across the Public/Private Divide*, 72 FLA. L. REV. 451 (2020); Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AMER. CRIM. L. REV. 109 (2020); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*", 42 DUKE L.J. 727, 738 tbl.1 (1993) (bank records).

[21] *See infra* note 125.

[22] United States v. Miller, 425 U.S. 435, 443 (1976) (finding no expectation of privacy in a customer's bank records).

[23] Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

[24] *See, e.g.*, *Miller*, 425 U.S. at 443 (bank records); *Smith*, 442 U.S. at 744 (call records).

[25] 565 U.S. 400 at 413–31 (2012).

by a total of five Justices suggested that the aggregation of many pieces of public location information by means of electronic tracking might give rise to a privacy expectation.[26] The Court went on to carve out a technology-sensitive rule in *Riley v. California*, holding that the otherwise broadly permissive search incident-to-arrest doctrine did not allow for warrantless searches of cell phones, even though police could search other personal effects without a warrant.[27] Finally, the Court's response to the digital revolution reached the third-party doctrine in *Carpenter v. United States*.[28] There, the Supreme Court held that the Fourth Amendment protection extends to law enforcement searches of historical cell-site location information stored by phone providers, exempting these data from the third-party doctrine.[29] Using cell phone location data for criminal investigations therefore required a warrant.[30]

In *Carpenter*, Chief Justice Roberts noted two ways in which cell phone location data is not like the kinds of information discussed in prior cases. First, he explained that the conveyance of location information to cell phone providers was not really "voluntary" because cell phones connect to towers automatically and carrying a cell phone is "indispensable to participation in modern society."[31] Second, Roberts emphasized the uniquely revealing nature of historical cell location data.[32] Cellular location data is generated

---

[26] For discussions of the logic of the concurring opinions, see for example Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, SUP. CT. REV. 205, 207–09 (2015); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 334 (5th ed. 2015) ("Both concurring opinions, involving five justices, embraced a new theory of privacy. In previous cases, the Court has focused extensively on whether something . . . was exposed to the public. The concurrences recognize that extensive and aggregated surveillance can violate a reasonable expectation of privacy regardless of whether or not such surveillance occurred in public."); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) ("The concurring opinions in *Jones* raise the intriguing possibility that a five-justice majority of the Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection.").

[27] Riley v. California, 573 U.S. 373, 399–401 (2014). The search incident-to-arrest doctrine would allow an extensive search of any other possessions on the person of the arrestee. *Id.* at 400 (mentioning bank statements, photos, wallets, etc.).

[28] 138 S. Ct. 2206 (2018).

[29] *See id.* at 2217. Cell-site location information is created when cell phones connect to cell towers, which modern phones do extremely frequently. This information can be used to pinpoint the location of the phone to a moderate degree of precision. *See id.* at 2219 (suggesting that companies could then locate a phone within 50 meters, with increased accuracy likely over time).

[30] *Id.* at 2221.

[31] *Id.* at 2220.

[32] *See id.* at 2216–17.

every time a phone connects to a cell tower, which modern devices do continuously, and therefore this data can be a moment-by-moment catalogue of a cell phone user's movements.[33]

Carpenter establishes that at least some uses of cell phone location information will count as searches under the Fourth Amendment. But Roberts specifically reserved the questions of real-time cellular location monitoring and "tower dumps," downloads of information on all the devices that connected to a particular cell-site during a particular interval because they are potentially less intrusive.[34] So those uses may, or may not, be searches.

Carpenter may also indicate that other business records are now due Fourth Amendment protection. Specifically concerning Part II's scenarios,[35] Matthew Kugler and Meredith Hurley explained how the rise of smart meters for the tracking of electrical power consumption has fundamentally changed the privacy interests at stake in utility records.[36] Utility companies now may gather thousands of datapoints a month about a person's energy usage, allowing them to accurately deduce many things about the activities occurring in the protected space of the home.[37] This arguably makes a warrant requirement for law enforcement use of smart meter data appropriate under *Carpenter* despite the clear pre-2010 case law denying Fourth Amendment protection.[38] This same reasoning can be used to question whether the failure to protect bank records is viable under *Carpenter's* logic given the changes in credit card usage since the 1970s.[39] Bank records may be useful in the pandemic context as they would reveal patterns of movement and purchases. Courts have not yet reached these questions, however, and they do not seem likely to do so in the near future.

The other two scenarios in Part II (drones and facial recognition) concern privacy in public spaces.[40] In general, the Court does not recognize a person's right to privacy from government observation when they are on

---

[33] *See id.* at 2211.

[34] *Id.* at 2220.

[35] *See infra* note 125.

[36] Kugler & Hurley, *supra* note 20, at 460–74.

[37] *Id.* at 469–74.

[38] *Id.* at 485–92; *but see* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527–28 (7th Cir. 2018) (finding an expectation of privacy in smart meter data under *Carpenter* but holding that installing and collecting data from smart meters was a reasonable regulatory search).

[39] Kugler & Hurley, *supra* note 20, at 487–89.

[40] *See infra* note 125.

public streets.[41] This is true whether a police officer is standing on a public street and sees into a person's yard, or whether the government installs a camera on a utility pole with the same view.[42] Even observation from low-flying aircraft to see into areas obscured from street-level view has been held to not be a search under the Fourth Amendment.[43]

These cases predate the rise of easy electronic video recording and facial recognition, however.[44] Some courts have questioned whether prolonged use of pole cameras to observe private property raises Fourth Amendment issues under *Jones*,[45] which was about prolonged GPS monitoring of a car on public streets, but so far this is a minority view.[46]

Some scholars have also raised concerns about the combination of public cameras and facial recognition technology. Andrew Ferguson, for example, believes that the *Jones-Riley-Carpenter* line of cases supports a series of principles that he applies to require limited Fourth Amendment protection against facial recognition.[47] Specifically he thinks that universal and pervasive facial recognition surveillance implicates Fourth Amendment

---

[41] California v. Ciraolo, 476 U.S. 207, 213 (1986) (stating that there is no expectation of privacy in that which can be seen from a public vantage point).

[42] United States v. Knotts, 460 U.S. 276, 282 (1983) (noting that "[n]othing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afford[s] them . . . .").

[43] *See* Florida v. Riley, 488 U.S. 445, 450–51 (1989); *Ciraolo*, 476 U.S. at 213–14.

[44] *See generally* Ferguson, *supra* note 20 (discussing the privacy implications of growing facial recognition use by the government) and Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107 (2019) (discussing private uses).

[45] *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 251 ("This type of surveillance provokes an immediate negative visceral reaction: indiscriminate video surveillance raises the spectre of the Orwellian state."); *see also* Order Granting Defendant's Motion to Suppress at 20, United States v. Vargas, No. CR-13-6025-EFS (E.D. Wash. Dec. 15, 2014) (similarly distinguishing prolonged video monitoring because it "is so different in its intrusiveness that it does not qualify as a plain-view observation."); United States v. Anderson-Bagshaw, 509 F. App'x 396, 405 (6th Cir. 2012); State v. Jones, 903 N.W.2d 101, 113–14 (S.D. 2017) (holding that pole camera surveillance of a front yard for two months is a Fourth Amendment violation).

[46] *See, e.g.*, United States v. Kay, 2018 WL 3995902, at *1, 3 (E.D. Wis. Aug. 21, 2018) (holding that 87 days of video surveillance is not a search under *Carpenter*); United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016), *cert. denied*, 137 S. Ct. 567 (2016); *see also* United States v. Cantu, 684 F. App'x 703, 703 (10th Cir. 2017); United States v. Brooks, 911 F. Supp. 2d 836, 843 (D. Ariz. 2012) (holding that law enforcement's use of a pole camera for long-term surveillance did not violate Fourth Amendment protections).

[47] Ferguson, *supra* note 20 at 1129–40.

protection while more isolated use or use only in real time does not.[48] But thus far no court has reached this result.

The very technologies that are most directly relevant to pandemic surveillance, then, have a somewhat questionable status under the Fourth Amendment. *Carpenter* settles that historic cell-site location information is protected, however,[49] and that gives us some comfort in concluding that at least some pandemic surveillance will raise Fourth Amendment issues. Several of the other methods used for pandemic surveillance—utility records or facial recognition—may raise Fourth Amendment issues as well, but this would require some expansion of existing doctrine.

B. NON-LAW ENFORCEMENT SEARCHES UNDER THE FOURTH AMENDMENT

The question "what is a search?" operates the same under the Fourth Amendment for both the law enforcement and non-law enforcement contexts, but the consequences of concluding that an action is a search are different outside the traditional law enforcement context. For law enforcement, courts default to requiring a warrant based on probable cause (or one of the specific exceptions to the warrant requirement).[50] When the goal of a search is not criminal law enforcement, when it is a "special needs" search, however, courts appear to assume that it is less problematic and less intrusive to conduct surveillance.[51] Courts evaluating a non-law enforcement "search" therefore conduct a reasonableness balancing analysis that weighs the intrusiveness of the search against the expected government benefits of that search rather than requiring probable cause and a warrant.[52]

The basic logic is that there are non-law enforcement situations in which the Fourth Amendment warrant and probable cause requirements are "impracticable."[53] In these instances the warrant requirement may be relaxed, such that a lesser amount of individualized suspicion is required and judicial

---

[48] *Id.* at 1142 ("[P]rinciples point to this type of generalized surveillance (identifying everyone, everywhere, for all time) being deemed a search for Fourth Amendment purposes."); *id.* at 1146–47 ("Under a *Carpenter* analysis, one might imagine the Supreme Court allowing real-time scans in certain locations, under certain circumstances (special events, targeted locations). However, generalized use for suspicionless surveillance would run afoul of Fourth Amendment search principles.").

[49] *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[50] *See id.* at 2221.

[51] *See, e.g.*, Camara v. Mun. Ct., 387 U.S. 523, 530 (1967) ("We may agree that a routine inspection of the physical condition of private property is a less hostile intrusion than the typical policeman's search for the fruits and instrumentalities of crime.").

[52] *See, e.g.*, *Camara*, 387 U.S. at 536–37.

[53] *See, e.g.*, City of Ontario v. Quon, 560 U.S. 746, 756 (2010).

pre-approval is not necessary.[54] A search based on no individualized suspicion—a dragnet—may also be reasonable "[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion . . . ."[55]

Many special needs searches are of people who, by virtue of their status or activities, have reduced expectations of privacy. The canonical examples are public school students and government employees. "[S]tudents within the school environment have a lesser expectation of privacy than members of the population generally" and can be subjected to a variety of intrusions in the form of a search or seizure.[56] Student athletes have further reduced expectations, as they have voluntarily chosen to seek the benefits of an extracurricular program.[57] The Supreme Court has used similar logic in the government employment context. It has explained that the "operational realities of the workplace" make it unreasonable for public employees to expect the same level of privacy protections as everyday citizens.[58] Those government employees who have or are seeking positions of particular trust and confidence have further reduced expectations based on their voluntary pursuit of those positions.[59]

COVID-19 surveillance fits somewhat oddly among this class of searches. COVID-19 surveillance would necessarily apply to anyone who is or could become infected, meaning everyone is fair game. This is the opposite of the canonical special needs case, where some distinguishing factor is used to emphasize the reduced privacy expectations of the subject class relative to those of the general public.[60] With COVID-19, we are surveilling the general public.

---

[54] *See* Nat'l Fed'n of Fed. Emps. v. Vilsack, 681 F.3d 483, 489 (D.C. Cir. 2012) ("Even where the government claims 'special needs,' a warrantless search is generally unreasonable unless based on 'some quantum of individualized suspicion.'") (citing Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 624 (1989)).

[55] *Skinner*, 489 U.S. at 624.

[56] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 656–57 (1995) (quoting New Jersey v. T.L.O., 469 U.S. 325, 348 (1984) (Powell, J., concurring)).

[57] *Vernonia Sch. Dist.*, 515 U.S. at 657 (1995) (likening student athletes to a "closely regulated industry").

[58] O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

[59] *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 670 (1989) ("It is readily apparent that the Government has a compelling interest in ensuring that front-line interdiction personnel are physically fit, and have unimpeachable integrity and judgment.").

[60] *See, e.g.*, United States v. Biswell, 406 U.S. 311, 317 (1972) (upholding search and seizure in the context of a pawnshop selling firearms); United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974) (air passengers), *cited with approval in Nat'l Treasury Emps. Union*,

The closest parallel to this kind of dragnet surveillance among the traditional special needs cases comes from highway checkpoints. Though automobile ownership is widespread and travel by car is almost universal, [61] automotive travel has always been treated as a special case. Automobiles are held to be subject to reduced expectations of privacy not just from their various characteristics (ready mobility, large windows, travel in public spaces), but also due to the intrusive regulation imposed on them itself; people should know better (in the view of courts) than to expect privacy in such a regulated device.[62]

Suspicionless dragnet stops of drivers at checkpoints are constitutional under the right circumstances. First, such stops must be for purposes other than the detection of ordinary criminal wrongdoing.[63] When the purpose is general crime control—such as mass license and registration checks (*Edmond*)—the Court "decline[s] to suspend the usual requirement of individualized suspicion."[64] Second, these checkpoint stops must be brief. This is consistent with the comment in *Skinner* that the privacy intrusions of dragnet searches should be "minimal."[65] The Supreme Court has therefore approved sobriety checkpoints aimed at removing drunk drivers from the road (*Sitz*),[66] brief information-seeking stops searches for witnesses to a hit and run (*Lidster*),[67] and searches of vehicles near the national border to intercept undocumented migrants (*Martinez-Fuerte*).[68]

The emphasis on purposes beyond general crime control is also on display in one of the few special needs cases that is about public health:

---

489 U.S. at 675 n.3; Griffin v. Wisconsin, 483 U.S. 868, 874 (1987) (probationers); *In re* J.G., 701 A.2d 1260, 1274–75 (1997) (sex offenders being tested for HIV).

[61] *See* SARAH A. SEO, POLICING THE OPEN ROAD 118–20 (2019) (describing how the combination of automobiles and prohibition led to the first widespread encounters between law enforcement and everyday citizens); *id.* at 119 ("It was significant that Prohibition's offenders were not limited to the unsavory sort.").

[62] Illinois v. Lidster, 540 U.S. 419, 424–25 (2004); California v. Carney, 471 U.S. 386, 392 (1985) ("These reduced expectations of privacy derive not from the fact that the area to be searched is in plain view, but from the pervasive regulation of vehicles capable of traveling on the public highways.").

[63] City of Indianapolis v. Edmond, 531 U.S. 32, 37–38 (2000) ("[W]e have upheld certain regimes of suspicionless searches where the program was designed to serve 'special needs, beyond the normal need for law enforcement.' . . . In none of these cases, however, did we indicate approval of a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.").

[64] *Id.* at 44.

[65] Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 624 (1989).

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

[67] Illinois v. Lidster, 540 U.S. 419, 421 (2004).

[68] United States v. Martinez-Fuerte, 428 U.S. 543, 545 (1976).

Ferguson v. City of Charleston.[69] There, the Court held that drug tests of pregnant mothers were unreasonable given the policy's law enforcement purpose.[70] The public hospital in Charleston began testing the urine of pregnant women who were suspected of being cocaine users with the aim of directing them to substance abuse programs.[71] The hospital worked closely with law enforcement and notified them of patients who twice tested positive or who missed appointments with substance abuse counselors.[72] This was a stick to encourage compliance.[73] Key in this case was the problem of "unauthorized dissemination" to "third parties."[74] The hospital could run the tests if, in its medical judgment, they were wise and beneficial to the patients.[75] But it could not run them for the purpose of providing information to law enforcement without falling out of the special needs category.[76]

Applied to the COVID-19 context, these factors suggest that public health agents using something like cellular location data for contact tracing could fall within the special needs category; the purpose is not traditional law enforcement, and the warrant and probable cause requirements are completely impractical. The remaining question for this surveillance program is whether this special needs search is sufficiently "reasonable" to be constitutional as a dragnet, as was the case with some traffic stops.

Using that same cellular location information to enforce a quarantine, particularly a quarantine of the general population, is less likely to count as a special needs search. The purpose is public health rather than preventing the usual social ills that accompany crime, but this was also true in *Ferguson*.[77] The question would ultimately turn on how distinct the quarantine enforcement regime was from the traditional law enforcement objective of general crime control. If a quarantine enforcement regime turned into an exercise in mass citation writing, one could question whether the goal was sufficiently closely aligned to pandemic enforcement to fit within the special needs category.

---

[69] 532 U.S. 67 (2001).

[70] *Id.* at 83–85.

[71] *Id.* at 70.

[72] *Id.* at 72.

[73] *See id*.

[74] *Id*. at 78.

[75] *Id.* at 79–81 (distinguishing "this case from circumstances in which physicians or psychologists, in the course of ordinary medical procedures aimed at helping the patient herself, come across information that under rules of law or ethics is subject to reporting requirements . . . .").

[76] *Id.* at 83–85.

[77] *Id.* at 70.

C. REASONABLENESS BALANCING IN THE FOURTH AMENDMENT

Even once a search falls within this special needs exception, courts must still "balance the individual's privacy expectations against the Government's interests" to determine if the search is reasonable.[78] This inquiry is stressed to be a "context-specific" investigation of "the competing private and public interests advanced by the parties."[79] Courts must consider the nature of the privacy interest allegedly compromised by the search, "the character of the intrusion imposed" by the government, and "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them."[80]

The Court has weighed these factors in several distinct ways. First, the Court has often emphasized the degree of intrusion present in special needs searches. In a case about student athlete drug testing, the Court emphasized that the actual collection of the urine sample was relatively inoffensive, with athletes forced into no greater exposure than was common in communal restrooms.[81] It specifically called the privacy interests "negligible."[82]

Furthermore, in one case on public employee drug testing, the Court noted several important limitations that added to the reasonableness of the search by limiting its intrusiveness.[83] Only employees tentatively accepted for promotion for one of three specified categories of jobs were tested, applicants knew in advance that drug tests were a requirement for promotion, and, as in the student athlete case, there was no direct observation of the urination and the test was for limited types of drugs.[84] The Court even remanded the case for further fact finding to determine whether the testing program was overbroad, covering employees who would not likely gain access to sensitive information and therefore should have been outside the scope.[85]

The Court found intrusion to be minimal in several other non-drug related cases as well. When the Court approved the warrantless investigation of a police officer's pager messages, it noted that the investigator had redacted the contents of any message that the officer sent while off duty.[86] In

---

[78] *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665–66 (1989).

[79] Chandler v. Miller, 520 U.S. 305, 314 (1997).

[80] Klayman v. Obama, 957 F. Supp. 2d 1, 38 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015) (quoting Bd. of Educ. v. Earls, 536 U.S. 822, 830–34 (2002)).

[81] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 658 (1995) (males observed from back, females had private stall).

[82] *Id.*

[83] *Nat'l Treasury Emps. Union*, 489 U.S. at 672 n.2.

[84] *Id.*

[85] *Id.* at 678.

[86] City of Ontario v. Quon, 560 U.S. 746, 762 (2010).

several checkpoint cases it has found the intrusion permissible because it is "slight."[87] In *Lidster*, it permitted stops because the "[c]ontact with the police lasted only a few seconds" and it was "less likely to provoke anxiety or to prove intrusive" given that the officers were seeking witnesses to a crime rather than suspects.[88]

In contrast, courts have been more skeptical in cases where the intrusion is severe. In the border search context, for instance, reasonable suspicion is required for more invasive searches like body cavity and strip searches.[89] But reasonable suspicion is not required for even extensive searches of non-private physical objects. In one case, the Supreme Court upheld a border search of a car's gas tank—which required substantial dismantling—on the grounds that it was not an especially private space when compared to a passenger compartment.[90]

This is not to say that the Court has insisted on full intrusion minimization. "This Court has 'repeatedly refused to declare that only the "least intrusive" search practicable can be reasonable under the Fourth Amendment.'"[91] Such a rule could be expected to create great problems "because 'judges engaged in *post hoc* evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished.'"[92]

Another major factor in these cases is the potential for arbitrary or abusive enforcement. The Court is wary of "standardless and unconstrained discretion" on the part of low-level government agents and prefers programs in which "the discretion of the official in the field be circumscribed, at least to some extent."[93] It is precisely to restrain such discretion that the warrant process involves a disinterested magistrate, who can shield citizens from

---

[87] *See e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451–52 (1990).

[88] Illinois v. Lidster, 540 U.S. 419, 425, 427 (2004).

[89] *See* Tabbaa v. Chertoff, 509 F.3d 89, 98 (2d Cir. 2007) (observing that strip and body cavity searches generally require reasonable suspicion); United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994) (concluding that strip and body cavity searches at the border go "beyond the routine"); United States v. Johnson, 991 F.2d 1287, 1292 (7th Cir. 1993) (noting that strip and body cavity searches are intrusive and "non routine").

[90] *See* United States v. Flores-Montano, 541 U.S. 149, 154 (2004).

[91] *Quon*, 560 U.S. at 763 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995)).

[92] *Id.* (quoting Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 629 n.9 (1989)).

[93] Delaware v. Prouse, 440 U.S. 648, 661 (1979) (determining a checkpoint regime to be unreasonable).

potential abuse.[94] When the Court upheld the regulatory search of a firearms dealer, it specifically noted that "the possibilities of abuse and the threat to privacy are not of impressive dimensions," the scope of the inspection being determined in part by a specific statute. [95] This concern with unfettered discretion is in part what motivates Christopher Slobogin's call for greater *ex ante* legislative and administrative involvement in what he terms "panvasive" surveillance.[96] Given that the police are playing an effectively policy-making role, he would ask that the police follow the usual rules of administrative agencies when creating surveillance regimes.[97]

The Court also considers whether the enforcement regime is likely to work. In a driver's license checkpoint case, it was skeptical that the described process would actually detect unlicensed drivers.[98] It therefore concluded that the spot checks were not "sufficiently productive to qualify as a reasonable law enforcement practice under the Fourth Amendment" even though the intrusion on individual drivers was "limited in magnitude."[99] The Court does not, however, insist that a policy be optimal. The choice among "reasonable alternatives remains with the" other branches of government.[100]

Finally, the Court has emphasized that it is fundamentally conducting a balancing exercise. Though the cases speak of "compelling state interests," "the phrase describes an interest that appears *important enough* to justify the particular search at hand, in light of other factors that show the search to be relatively intrusive upon a genuine expectation of privacy."[101] A less intrusive search requires a more limited justification and a more intrusive search a more extensive justification. "[T]he measures adopted . . . [must be] reasonably related to the objectives of the search and not excessively intrusive in light of" the objective.[102]

---

[94] Camara v. Mun. Ct., 387 U.S. 523, 532–33 (1967) ("This is precisely the discretion to invade private property which we have consistently circumscribed by a requirement that a disinterested party warrant the need to search.").

[95] United States v. Biswell, 406 U.S. 311, 317 (1972) (upholding search and seizure in the context of a pawnshop selling firearms).

[96] Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 118–20 (2016).

[97] *Id.* at 120–22.

[98] *Prouse*, 440 U.S. at 660.

[99] *Id.* at 660–61.

[100] Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 453–54 (1990).

[101] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 661 (1995); *see also* O'Connor v. Ortega, 480 U.S. 709, 719–20 (1987) ("In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.").

[102] *O'Connor*, 480 U.S. at 726 (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985)).

II. TWO EMPIRICAL STUDIES OF PANDEMIC SURVEILLANCE ATTITUDES

As shown in Part I, more intrusive searches require greater justification and greater regulation. There are many ways to quantify the degree of intrusion, but one approach is to simply ask people how much they object. Do people, when confronted with the prospect of pandemic surveillance, perceive government's actions as highly intrusive?

Many scholars have advocated using public opinion data to inform the Fourth Amendment analysis.[103] Christopher Slobogin and Joseph Schumacher pioneered this method by having respondents rate the intrusiveness of a variety of law enforcement information gathering techniques.[104] Though they largely found respondents' opinions typically track judicial conclusions about whether the technique at issue constitutes a "search" under the Fourth Amendment, scattered and important divergences do arise.[105] Similarly, work by Christine Scott-Hayward and colleagues and Bernard Chao and colleagues has investigated Americans' opinions and beliefs about forms of electronic surveillance, finding, for example, that people do generally expect privacy in data like their cell phone location records.[106]

This method was used by Matthew Kugler in an analysis of border searches of electronic devices.[107] The government has extensive power to conduct searches of people crossing the national border, including physical packages of all sorts.[108] It was very unclear at the time of the article whether the extremely permissive border search doctrine would allow an unfettered

---

[103] For an extensive discussion justifying the use of such data, *see* Kugler & Strahilevitz, *supra* note 26, at 224–44.

[104] *See* Slobogin & Schumacher, *supra* note 20, at 737–39; CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 111 (2007); *see also* Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 343–44 (2009) (replicating Slobogin and Schumacher's main results in a more representative sample).

[105] *See* Slobogin & Schumacher, *supra* note 20, at 739–40, 738 tbl.1 (noting that the use of a secretary as an undercover agent is deemed noticeably more intrusive by respondents than the search of an office drawer).

[106] Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 45–58 (2015); Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 297–315 (2018).

[107] Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1166–67 (2014).

[108] *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 150–52 (2004).

examination of electronic devices as it did more traditional parcels.[109] The data from this study showed that people considered searches of the contents of their electronic devices to be as intrusive as strip searches, and even more likely than strip searches to reveal sensitive personal information.[110] These results supported greater regulation of such searches.

Matthew Kugler and Lior Strahilevitz have also shown that people's privacy expectations are relatively stable over time. Specifically, people's privacy expectations shifted only a small amount and only temporarily after a major and well-publicized Supreme Court ruling extended privacy protection to electronic devices in the context of an arrest.[111]

Extending this tradition of Fourth Amendment scholarship into the pandemic surveillance context, two samples of American adults were recruited by Dynata, an online survey firm with an established panel.[112] The demographics of the samples were set to match U.S. census proportions on the dimensions of age, sex, region, education, and race/ethnicity. Full demographics are reported in the Appendix. The first sample contained 1,178 individuals.[113] Data were collected on April 9th, 10th, and 13th, 2020. On those three days, a total of 6,188 American deaths were attributed to COVID-19, for a total count of 28,140 for the pandemic to that point.[114] Data for the second sample of 1,197 were collected on June 18th, 19th, and 20th. On those

---

[109] In the wake of Riley v. California, 573 U.S. 373, 402–03 (2014) (creating an electronic search exception to the search incident-to-arrest doctrine), it seems likely that there would be an electronic device exception to the border search doctrine..

[110] Kugler, *supra* note 107, at 1197 tbl.1A, 1198 tbl.1B, 1199.

[111] *See* Matthew B. Kugler & Lior J. Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747, 1780 (2017) (showing that privacy expectations in electronic devices increased slightly one week after the ruling but had returned to baseline one year later. Privacy expectations in physical searches—not covered by the ruling—did not change).

[112] *About*, DYNATA, https://www.dynata.com/about-us/ [https://perma.cc/RW7S-VTZS] (last visited June 29, 2021).

[113] For both samples, inattentive participants were screened in two ways. First, participants who did not give the appropriate response to either of two attention check questions—questions asking participants to give a particular response—were unable to complete the study. Second, participants were screened from the final sample if they finished the study in less than one-third of the time taken by the median participant or gave comments on the final question indicating a lack of attention. The second sample also included a CAPCHA question.

[114] 2,161, 2,290, and 1,737 respectively according to *United States Coronavirus*, WORLDOMETER, https://www.worldometers.info/coronavirus/country/us/ [https://perma.cc/9HZV-J854] (last visited July 28, 2021).

three days, a total of 2,094 American deaths were attributed to COVID-19, for a total of 125,443 from the pandemic to that point.[115]

These two samples were intended to capture two distinct moments in the lifecycle of the pandemic. The first data collection occurred during the height of the first peak.[116] Individuals in Wave 1 reported being substantially affected and concerned by COVID-19. Large majorities said they were avoiding large gatherings (87.1%), mass transit and air travel (84.7%), small gatherings (78.3%), and public places (77.2%). Most (64.9%) said they had been following stay-at-home guidance for three or more weeks, going out only for necessary errands like groceries or to work in an essential industry.[117] Though only 13.3% said they believed that they or a close friend or family member had already been infected, many were either very (37.7%) or somewhat (38.2%) worried that they or someone in their family would be exposed to COVID-19.[118] Notably, these questions about COVID-19 experiences followed, rather than preceded, the main study measures that are described below.

Wave 2 data were collected well after the death toll had exceeded 100,000.[119] Daily death rates had substantially fallen from the peak, states had begun to reopen, and the infection rate had begun to rise again.[120] The members of this sample had ample opportunity to become familiar with COVID-19. Somewhat fewer reported avoiding large gatherings (79.4%), mass transit and air travel (75.9%), small gatherings (61.0%), and public places (62.7%). Though more reported they or a close friend or family member had been infected (18%), they were somewhat less likely to be very (28.7%) or somewhat (41.7%) worried that they or a family member might be exposed. Importantly, Wave 2 also occurred after the height of the Black Lives Matter protests sparked by the death of George Floyd. This moment in time was therefore also relevant to the law enforcement baseline measures as those mass protests might affect views of regular police surveillance.

---

[115] *Id.* 769, 747, 578, respectively. As the last day was a Saturday, the number of deaths reported was lower for that day.

[116] *See* WORLDOMETER, *supra* note 114, for a chart of deaths per day.

[117] Eighteen and one half percent had been doing so for 2 weeks, 6.3% for one week, 4.1% for less than a week, and 6.3% said they were not following stay-at-home guidance.

[118] Seventeen and seven-tenths percent were not too worried and 6.5% were not worried at all.

[119] WORLDOMETER, *supra* note 114.

[120] For a review of which restrictions were in place in which states at which times, *see, e.g.*, Lindsay K. Cloud, Katie Moran-McCabe, Elizabeth Platt & Nadya Prood, *A Chronological Overview of the Federal, State, and Local Response to COVID-19*, *in* ASSESSING LEGAL RESPONSES TO COVID-19 10, 10–16 (Scott Burris, Sarah de Guia, Lance Gable, Donna E. Levin, Wendy E. Parmet & Nicholas P. Terry eds., 2020).

A. POPULAR ATTITUDES TOWARD COVID-19 SURVEILLANCE

In each wave, participants were asked to report their attitudes about surveillance conducted in one of three different domains: (1) law enforcement officers collecting information for traditional crime-fighting purposes, (2) law enforcement officers collecting information to ensure compliance with COVID-19 stay-at-home orders, and (3) public health officials (rather than law enforcement) collecting information to track COVID-19 infections. This contrasted the two different kinds of COVID-19 surveillance generally contemplated with traditional law enforcement.

Each participant was randomly assigned to one of these three scenarios/contexts, and the participant then had this context repeatedly reinforced throughout. In the traditional police context, for example, the overall instructions read:

> The government collects information for a variety of purposes. For the questions on the next pages, please think about **police officers** conducting investigations **in the normal course of their duties**. Their goals in these investigations are the **general prevention and investigation of crimes**. To fulfill these goals, they would be seeking information about the locations and movements of both criminal suspects and victims.[121]

In contrast, the public health agent instructions read:

> The government collects information for a variety of purposes. For the questions on the next pages, please think about **public health officials** working on behalf of the government to **track the spread of a highly infectious disease,** such as the coronavirus disease, otherwise known as COVID19. Their goal in these investigations is the **promotion of public health**. To fulfill this goal, they would be seeking information about the locations and movements of people known to be infected and those with whom they may have come into contact.

This difference was then further emphasized at the start of each search vignette, "As part of a police investigation, an officer . . . " versus "As part of a public health investigation, a public health agent . . . " and "To examine compliance with stay-at-home orders, a police officer . . . ."

These three variants capture an important set of distinctions under American law. As discussed in Part I, searches for traditional law enforcement purposes are treated very differently than searches conducted for non-law enforcement purposes. These vignettes contrast the traditional law enforcement scenario with a "public health" variant, which has no punitive purpose and does not involve traditional law enforcement in any way, and a quarantine enforcement variant, which combines both traditional law enforcement and public health monitoring.

---

[121] These instructions were displayed for a minimum of 10 seconds before the participant could advance to the next screen.

The types of surveillance used here were inspired by those discussed contemporaneously in relation to COVID-19. The heavy emphasis was on the use of cell phone location data, either by law enforcement or public health officials, to track movements and contacts. Participants were also asked about the use of facial recognition technology in conjunction with public surveillance cameras, smart meter data, drones, and credit card records. These searches were presented on separate screens in random order.

For each surveillance method, participants were asked three questions. First, they rated whether the search "violated a reasonable expectation of privacy" on a scale ranging from Definitely Not (1) to Definitely Yes (5). Then they rated the intrusiveness of the search on a sliding scale ranging from 0 – Not at all Intrusive to 100 – Extremely Intrusive.[122] Finally, they were asked whether the government official in question (police or public health agent) should be legally allowed to look for information this way without a warrant or court order (Yes or No).

This article presents the results of Wave 1 first. In that wave, results across these three measures were extremely similar. This article uses average intrusiveness, expectation of privacy, and warrant scores to allow for tests of the overall effects. These tests show that traditional law enforcement searches were viewed as less intrusive and less violative of expectations of privacy than searches conducted for COVID-19 purposes, and participants were less likely to prefer that a warrant or court order be required for these traditional law enforcement purposes.[123] The two pandemic conditions did not significantly differ from each other.

Looking at the individual searches on the two continuous dependent measures—the intrusiveness and expectation of privacy questions—shows the consistency of this pattern.[124] As can be seen in Figure 1, the overall effect

---

[122] The reasonable expectation of privacy question is repeated from prior work by Kugler and Strahilevitz, *supra* note 26 at 209–11. The intrusiveness question was first used by Slobogin and Schumacher, *supra* note 20, at 736.

[123] Intrusiveness: $F(2, 1175) = 25.10$, $p < .001$ $\eta^2 = .041$. Law Enforcement (LE) ($M = 59.06$, $SD = 25.42$) was significantly lower than Public Health (PH) ($M = 70.87$, $SD = 23.28$), and LE-Stay-at-Home ($M = 68.35$, $SD = 24.63$), which did not differ.

Expectation of privacy: $F(2, 1175) = 37.94$, $p < .001$ $\eta^2 = .061$. LE ($M = 3.20$, $SD = 1.03$) was significantly lower than PH ($M = 3.77$, $SD = 0.96$), and LE-Stay-at-Home ($M = 3.70$, $SD = 1.03$), which did not differ.

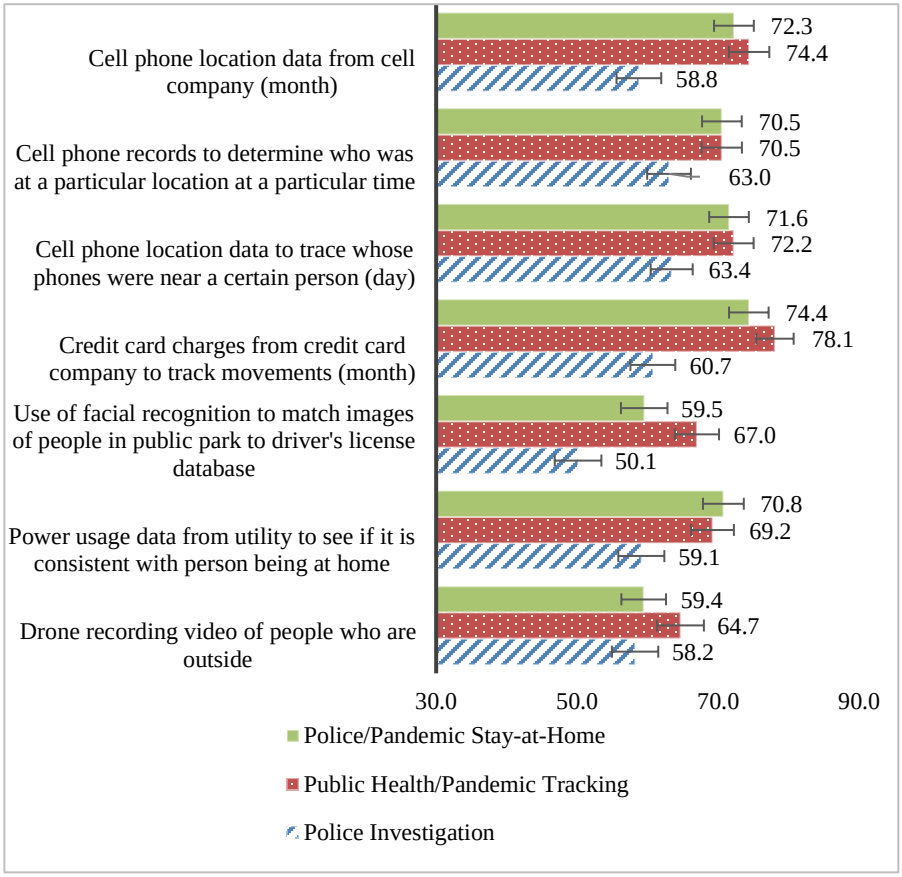
Warrant: $F(2, 1175) = 7.31$, $p < .001$ $\eta^2 = .012$. LE ($M = 0.62$, $SD = 0.34$) was significantly lower than PH ($M = 0.69$, $SD = 0.34$), and LE-Stay-at-Home ($M = 0.71$, $SD = 0.32$), which did not differ.

[124] ANOVAs and post hoc tests on these measures yielded identical results. $F(2, 1175) > 4$ for all omnibus tests. For all cases except the park and drone vignettes, Bonferroni-corrected post hoc tests ($p < .05$) revealed that the law enforcement condition had significantly lower mean scores than the other two, which did not differ significantly. For the park vignette, law

of law enforcement searches being seen as significantly less intrusive holds true for almost all of the search scenarios. Traditional law enforcement is always lower than the other two conditions – public health and law enforcement public health surveillance - and is significantly lower than both for all searches except the drone scenarios. For the drone, traditional law enforcement is still significantly lower than the public health condition but is not significantly lower than the law enforcement stay-at-home order condition.

enforcement was significantly lower than public health law enforcement, which in turn was significantly lower than the general public health condition. For drone, law enforcement was significantly lower than public health, but public health law enforcement did not differ significantly from either.

Figure 1: Perceived intrusiveness of searches in different contexts



Notes: Error bars depict 95% confidence intervals.[125] Responses range from 0 – Not at all Intrusive to 100 – Extremely Intrusive. Table of means and standard deviations is in the Appendix.

[125] After the introductory phrase, which varied by condition (e.g., "As part of a police investigation, an officer . . . "), the questions read as follows:

. . . obtains from a cell phone company a record of a phone's movements over the course of 4 weeks.

. . . obtains from a cell phone company a record of everyone whose phone was near a particular place at a particular time.

. . . obtains from a cell phone company a record of everyone whose phone was near a particular other person's phone throughout a day, with the goal of determining with whom that person may have come into contact.

. . . obtains from a credit card company a list of all charges made on a person's credit card over a month-long period, to determine where the user has been going and whom the user may have been with.

Table 1 shows that this same pattern was reflected on the expectation of privacy measure. People consistently viewed pandemic surveillance as more violative than traditional law enforcement surveillance. Comparing the scores from the public health condition in this study to some past data, it rapidly becomes clear that people are extremely concerned about pandemic surveillance efforts by the state. Table 2 (in the next section) reprints some data from a 2015 data collection by Kugler and Strahilevitz about law enforcement surveillance.[126] The top two searches from that dataset were remotely turning on a person's webcam (4.06 on a 5-point scale) and obtaining their emails from their ISP (3.73). Only 2 of the 7 pandemic surveillance searches in this study fell under those two top scores.

. . . uses facial recognition to identify people who were outside in a public park at a particular time. The officer uses a program to compared images captured by a security camera in the park to those in the state's driver's license database.

. . . obtains from a utility a house's smart meter information, checking to see whether the house's electricity usage throughout the day is consistent with a person being at home.

. . . operates a drone with a camera attached to it to fly outside and video record anyone who is out on the streets.

[126] Kugler & Strahilevitz, *supra* note 26, at 252–55.

Table 1: Whether searches violate reasonable expectations of privacy

	Police investigation	Public Health/ Pandemic	Police/ Stay-at-home
Cell phone location data tracking a phone's movements (month)	3.13_a (1.43)	3.92_b (1.25)	3.89_b (1.27)
Cell phone records of who was at a particular location at a particular time	3.41_a (1.39)	3.77_b (1.28)	3.77_b (1.35)
Cell phone location data to trace whose phones were near a certain person (day)	3.36_a (1.35)	3.81_b (1.25)	3.80_b (1.32)
Credit card charges from CC company to track movements (month)	3.25_a (1.41)	4.09_b (1.21)	4.01_b (1.25)
Use facial recognition to match images of people in public park	2.77_a (1.41)	3.60_c (1.35)	3.33_b (1.43)
Power usage data from utility to see if consistent with person at home	3.28_a (1.44)	3.76_b (1.30)	3.75_b (1.38)
Drone recording video of people who are outside	3.18_a (1.41)	3.48_b (1.47)	3.35_{ab} (1.42)

Notes: Means not sharing subscripts differ significantly at the $p < .05$ level. Numbers in parentheses are standard deviations. Responses range from 1 – Definitely Not to 5 – Definitely Yes.

Despite this study being conducted during the peak of an international pandemic, people were still resistant to these non-law enforcement searches, and in fact were more resistant to them than the same searches being conducted by law enforcement for ordinary crime prevention purposes.

When the study was repeated in mid-June—approximately 100,000 American COVID-19 deaths later—the results were basically identical. Using the overall measures for the intrusiveness, expectation of privacy, and warrant scores produced the same effect of search context, law enforcement searches were seen as less intrusive, less violative of expectations of privacy, and needed less court supervision.[127] But there were no significant

[127] Effects within Wave 2. Intrusiveness: $F(2, 1194) = 42.32$, $p < .001$ $\eta^2 = .066$. Law Enforcement (LE) ($M = 56.32$, $SD = 26.08$) was significantly lower than Public Health (PH) ($M = 70.12$, $SD = 23.00$), and LE-Stay-at-Home ($M = 70.00$, $SD = 24.05$), which did not differ.

differences between waves, and no interaction between wave and condition, on either the overall scores or on any of the individual expectation of privacy or intrusiveness measures.[128] This means that views of both pandemic-related searches and traditional law enforcement searches did not change despite the events of the intervening two months. Full data on both expectations of privacy and intrusiveness for this wave are presented in the Appendix.

In the second wave, participants were asked two follow-up questions specifically about COVID-19 surveillance. For one, participants selected from a list the statement or statements that best captured their views of COVID-19 cell phone location surveillance.[129] No single option attracted majority support. The most commonly chosen alternative expressed concern that the location data would be used for other things (48.2%), with many also saying that they did not trust the government with the information (40.6%). Only about a quarter (24.1%) said that they were concerned the information would be shared with law enforcement, however, and only 20.0% cited cost of such surveillance efforts as a concern. Participants also expressed some skepticism about the efficacy of cell phone location surveillance. More people said that cell phone tracking would not reduce the spread (34.5%) of COVID-19 than said that it would (22.3%), and only 13.5% said that tracking would help the country open faster.

The second question asked participants specifically about their views of the efficacy of cell phone tracking for control of COVID-19.[130] Only about a quarter thought that the tracking would be "extremely" (10.6%) or "very"

Expectation of privacy: $F(2, 1194) = 46.05$, $p < .001$ $\eta^2 = .072$. LE ($M = 3.17$, $SD = 1.04$) was significantly lower than PH ($M = 3.77$, $SD = 0.93$), and LE-Stay-at-Home ($M = 3.73$, $SD = 1.01$), which did not differ.

Warrant: $F(2, 1194) = 6.05$, $p = .002$ $\eta^2 = .010$. LE ($M = 0.64$, $SD = 0.36$) was significantly lower than PH ($M = 0.70$, $SD = 0.34$), and LE-Stay-at-Home ($M = 0.72$, $SD = 0.33$), which did not differ.

[128] Intrusiveness. Wave effect: $F(1, 2369) = 0.38$. Interaction between wave and context: $F(2, 2369) = 1.62$.

Expectation of privacy. Wave effect: $F(1, 2369) = 0.00$. Interaction between wave and context: $F(2, 2369) = 0.22$.

Warrant. Wave effect: $F(1, 2369) = 0.63$. Interaction between wave and context: $F(2, 2369) = 0.18$.

[129] This question was asked of all participants, and there were no differences based on whether the participants had previously been rating law enforcement, public health, or law enforcement stay-at-home order scenarios. The explanations were presented in random order. In addition to the reported results, 3% also selected the "Other" option and included their own explanation.

[130] "Imagine the government tracked people using their cell phone location information to help limit the spread of COVID-19. How effective do you believe this tracking would be at controlling the virus?" Responses ranged from 1 – Not at all effective to 5 – Extremely effective. This question was also asked of all participants.

(12.4%) effective, with a further third (32.0%) saying that it would be "moderately" effective. Many expressed skepticism, saying that tracking would be only "slightly effective" (19.3%) or "not effective at all" (25.7%).

B. COMPARISON OF LAW ENFORCEMENT SEARCH ATTITUDES OVER TIME

A recurrent question in this domain is whether the surveillance attitudes that we observe are stable over time. The data in the previous section documents an impressive amount of stability in attitudes over the span of three extremely tumultuous months—recall that participants experienced both the rising COVID-19 death toll and the mass protests of early June before Wave 2 of the survey. But there is a valid concern that the mere beginning of the pandemic also had some effect on attitudes, and that this occurred before Wave 1 of the present project. One could imagine, for instance, the beginning of a pandemic might depress privacy concerns across the board. This would be consistent with psychological work showing that feelings of threat and thoughts of death cause meaningful changes in political attitudes and beliefs.[131]

Though there are no prior data on public health surveillance that would permit a direct comparison with the present results, data collected by Kugler and Strahilevitz in May and June 2015 allows for a comparison on several law enforcement measures.[132] In Wave 1 of the present survey, these law enforcement questions were asked after the ones presented in the prior section and employed the 5-point reasonable expectations of privacy scale described above.

As can be seen in Table 2, it is not the case that privacy expectations have generally declined. In the 5 years from 2015 to 2020, expectations of privacy were mostly constant. The sum of the differences across the 10 search types included in this comparison is 0.10 on a 5-point scale, for an average change of 0.01. Expectations increased significantly for use of public

---

[131] *See, e.g.*, Brian L. Burke, Andy Martens & Erik H. Faucher, *Two Decades of Terror Management Theory: A Meta-Analysis of Mortality Salience Research*, 14 PERSONALITY & SOC. PSYCH. REV. 155, 185–87 (2010).

[132] Kugler & Strahilevitz, *supra* note 26, at 257, 260. For the 2015 data, N was 716 for the non-GPS questions and 362 for the GPS questions. The April 2020 data contain only those participants who were initially in the law enforcement condition in the first wave, N = 389. Those participants in the other two conditions had higher privacy expectations on some measures—consistent with their prior responses—and potentially presented a misleading picture of change over time on law enforcement expectations. These questions were omitted in the second wave to create room for the Black Lives Matter (BLM) items and supplemental questions on COVID-19.

cameras and facial recognition and barely changed on other measures.[133] Though it is obviously possible that there was a change in privacy expectations prior to COVID-19 and that COVID-19 had the effect of negating that change, it seems far more likely that expectations have instead remained constant during this time and that the emergence of the COVID-19 health crisis therefore had no noticeable effect.

Table 2 – Expectations of privacy against law enforcement searches by year

	May-June, 2015		April, 2020		Difference	
Remote activate webcam	4.06	(1.37)	3.90	(1.44)	-0.16	
Obtain Emails From ISP	3.73	(1.40)	3.64	(1.39)	-0.09	
Facial recognition at Super Bowl	2.61	(1.54)	2.87	(1.44)	0.26	*
Camera in public park	2.40	(1.55)	2.65	(1.51)	0.25	*
Cell-site data	3.26	(1.50)	3.32	(1.33)	0.06	
Stingray cell-phone tracking	3.42	(1.42)	3.53	(1.38)	0.11	
GPS-Locate	3.44	(1.50)	3.42	(1.36)	-0.01	
GPS-Track 1 day	3.55	(1.52)	3.48	(1.38)	-0.07	
GPS-Track 1 week	3.67	(1.46)	3.55	(1.35)	-0.12	
GPS-Track 1 month	3.73	(1.46)	3.61	(1.37)	-0.13	

Notes: Higher numbers indicate greater expectations of privacy on a 1–5 scale. Numbers in parentheses are standard deviations. ** indicates differences that are significant at the $p < .01$ level, * at $p < .05$. The questions appeared in random order except the GPS searches, which were last.[134]

[133] Given that there are 10 searches here, we performed a Bonferroni correction for multiple comparisons. Without that correction, the webcam difference would have been significant at the .05 level.

[134] Participants were asked, "Would it violate people's reasonable expectations of privacy if law enforcement . . .

. . . used remote activation software to turn on the webcam on their laptop without their permission?

. . . obtained from their internet service provider copies of emails exchanged between them and someone else?

. . . used facial recognition software to check whether any of the fans entering the Super Bowl stadium match images in a Department of Homeland Security database?

. . . installed a video camera to watch a public park where criminal activity has recently occurred?

. . . obtained from their cell-phone company stored information about whether their cell phone was near a particular location on a particular day?

In addition to showing that COVID-19 has not had a strong general effect on privacy attitudes, these results also help counter one criticism sometimes aimed at this type of work: that attitudes are too unstable to be the basis of legal doctrine. Over a five-year period, where much happened, expectations were stable. And expectations were again stable during the COVID-19 pandemic itself, as demonstrated in Section II.A, even as the social situation evolved, and a string of anti-law enforcement protests swept the entire country. This suggests that survey results in this area from one year will most likely carry over to the next.

C. UNDERSTANDING PUBLIC HEALTH SURVEILLANCE ATTITUDES

Pandemic surveillance worries different people than law enforcement surveillance. Intuitively, this should not be surprising. Though some people are opposed to "government" surveillance in general, not all types of government monitoring are concerning in the same ways. And these results show different ideological beliefs correlate with surveillance concerns in each context.

Prior work has observed that attitudes about law enforcement searches are correlated with the psychological construct known as rightwing authoritarianism.[135] The social psychological theory of authoritarianism defines authoritarians as people who are especially willing to submit to authority, who believe that it is particularly important to yield to traditional conventions and norms, and who are hostile and punitive toward those who question authority or who violate such conventions and norms.[136] The specific authoritarianism scale used in prior work, and again employed here, is the Authoritarian Submission scale. This scale is intended to measure the

. . . used a fake cell tower to trick their phone into giving the police more accurate information about where the phone is?

. . . used a car's onboard GPS system to locate it on public streets at a single moment in time without the owner's permission?

. . . used a car's onboard GPS system to track its movements on public streets for one day without the owner's permission?

Same, but for one week?

Same, but for one month?"

[135] Kugler & Strahilevitz, *supra* note 26, at 252–55.

[136] *See* Bob Altemeyer, *The Other "Authoritarian Personality," in* 30 ADVANCES IN EXPERIMENTAL SOC. PSYCH. 47 (Mark Zanna ed., 1998).

first of those impulses: the extent to which people believe that authority should be respected and obeyed rather than challenged and questioned.[137]

As can be seen in Table 3, attitudes about traditional law enforcement surveillance again correlated with authoritarianism on each of our three composite measures. Those scoring higher in authoritarianism perceived law enforcement searches to be less intrusive and less a violation of expectations of privacy and were less likely to want to require a warrant or court order to conduct them. Yet this effect was significantly weaker on each of the three measures in the public health agent condition, where authoritarianism did not predict any of them significantly. The law enforcement pandemic surveillance condition was intermediate between the other two conditions. Similar patterns were found on two questions that were added in the second survey wave, one on trust in police and one on support for the then-recent Black Lives Matter (BLM) protests. Higher trust in the police was correlated with viewing the searches as less intrusive and less a violation of expectations of privacy—and support for BLM with viewing them as more intrusive and more a violation—in the law enforcement condition, but not the public health condition. The pattern on the BLM question actually reversed in the public health condition; those who supported the protests more thought public health searches were slightly *less* intrusive.

Support for public health monitoring was correlated with different constructs. Trust in the police was irrelevant, and trust in public health officials was now relevant. Further, in the public health and law enforcement public health conditions, the specific belief that cell phone tracking would be effective in limiting the spread of COVID-19 was associated with viewing all searches as less intrusive and less a violation of expectations of privacy.

Probing deeper reveals an interesting pattern among these attitudinal measures. Trust in the police and trust in public health officials were themselves moderately related.[138] Nevertheless, authoritarianism correlated

---

[137] We measured this construct at the close of the survey section asking about COVID-19 surveillance. Scale items include "It's great that many young people today are prepared to defy authority" (reverse coded), and "What our country needs most is discipline, with everyone following our leaders in unity." The response scale ranged from 1 (strongly disagree) to 6 (strongly agree). Higher scores indicate stronger endorsement of authoritarian ideologies. John Duckitt, Boris Bizumic, Stephen W. Krauss & Edna Heled, *A Tripartite Approach to Right-Wing Authoritarianism: The Authoritarianism-Conservatism-Traditionalism Model*, 31 POL. PSYCH. 685, 690 (2010) ("Thus, the 'authoritarian submission' dimension can be defined as expressing attitudes favouring uncritical, respectful, obedient, submissive support for existing societal or group authorities and institutions (protrait) versus critical, questioning, rebellious, oppositional attitudes to them (contrait).").

[138] $r(1196) = 0.438$, $p < .001$.

strongly with trust in police, but not trust in public health officials.[139] Authoritarianism also negatively predicted support for the BLM protests.[140] This suggests that there is a general pro- (or con-) police sentiment that does not generally translate to views of government surveillance outside the traditional law enforcement context.

[139] Authoritarianism correlated with trust in police $r(1191) = 0.432$, $p < .001$ but not trust in public health officials $r(1191) = 0.051$, *ns*.

[140] $r(1186) = -0.464$, $p < .001$. Trust in the police is, unsurprisingly, also related negatively to support for the BLM protests $r(1192) = -0.323$, $p < .001$. Trust in public health officials is slightly positively related to BLM support, however. $r(1191) = 0.095$, $p < .001$.

Table 3: Correlations with attitudinal measures

Traditional Law Enforcement	Intrusiveness	Expectation of Privacy	Warrant
Authoritarianism	-.263 ***	-.262 ***	-.195 **
Trust in Police	-.266 ***	-.231 ***	-.344 **
Support for BLM	.200 ***	.166 ***	.036
Trust in Public Health Officials	-.079	-.060	-.172 **
Perceived Effectiveness COVID Cell Tracking	-.063	-.079	-.344 **
Worried Family Exposed to COVID	.082 *	.058	-.014

Public Health	Intrusiveness	Expectation of Privacy	Warrant
Authoritarianism	-.039	-.036	-.027
Trust in Police	.000	-.001	-.085
Support for BLM	-.125 *	-.065	-.183 **
Trust in Public Health Officials	-.163 ***	-.177 ***	-.264 **
Perceived Effectiveness COVID Cell Tracking	-.336 ***	-.360 ***	-.462 **
Worried Family Exposed to COVID	-.025	-.034	-.095 *

Law Enforcement - Stay-at-home	Intrusiveness	Expectation of Privacy	Warrant
Authoritarianism	-.098 **	-.112 ***	-.125 **
Trust in Police	-.109 *	-.137 ***	-.302 **
Support for BLM	.038	.040	.031
Trust in Public Health Officials	-.070	-.098	-.242 **
Perceived Effectiveness COVID Cell Tracking	-.273 ***	-.375 ***	-.455 **
Worried Family Exposed to COVID	-.035	-.042	.123 **

On one level, it is not surprising that public health monitoring should tap different psychological constructs than does law enforcement monitoring. But these patterns reflect the importance that people are placing on the government's motivation behind the search. Not only are people more accepting of some but not other government programs on average, but different people are more accepting depending on the purpose. As such, universal agreement on what types of government monitoring during a

pandemic are "reasonable" is unlikely. Nevertheless, universal agreement or not, courts will need to grapple with this question.

III. MAKING PANDEMIC SURVEILLANCE REASONABLE

Prior to these studies, not much was known about how the public viewed pandemic surveillance. In this Part, we apply our empirical results from Part II to the question of how best to think about pandemic searches from a legal standpoint. We then comment on the types of limitations and procedures that would make pandemic public health surveillance, especially cell phone location surveillance, more constitutionally reasonable.

A. HOW INTRUSIVE ARE PANDEMIC SEARCHES?

Central to the reasonableness balancing analysis is the intrusiveness of the proposed search. Courts have stressed that the proposed intrusion on privacy is "slight," "negligible," and lasting "only a few seconds," when approving searches while expressing great skepticism about searches that are overbroad or highly intrusive.[141] The data presented in Part II show that people feel the intrusiveness of many of these surveillance techniques quite acutely. In the law enforcement condition, more people felt that use of historical cell-site data violated their expectations of privacy (43.5%) than did not (31.9%).[142] The same for tower dumps (48% yes, 26.2% no) and cell contact tracing (47% yes, 26.2% no). This is, in fact, perfectly consistent with the high value Chief Justice Roberts has told us should be placed on cell phone location information.[143] But importantly this study tells us that people feel the invasion *more* acutely in the pandemic context. Those same proportions are exaggerated in the public health surveillance condition. For location history, 66.0% yes and 15.2% no. For tower dumps 59.1% yes, 17.9% no. For contact tracing 62.2% yes, 16.0% no.[144] This is not a small shift.

The central message of these results is that people find pandemic surveillance, either conducted by public health authorities or by police to enforce quarantine orders, to be more intrusive than traditional law

---

[141] *See supra* notes 82–90.

[142] Contrasting those who picked one of the two choices below the midpoint with those who picked one of the two choices above the midpoint on the reasonable expectation of privacy question. This analysis combines the data from Waves 1 and 2, for a total N of 2375.

[143] *See supra* notes 28–33.

[144] The numbers are approximately the same for the law enforcement stay-at-home enforcement condition. Location history: 15.0% no, 65.3% yes. Tower dump: 18.0%, no 59.8% yes. Contact tracing: 15.8%, no 63.2% yes. Full results are given in Table 5A in the Appendix.

enforcement surveillance. There are many potential reasons for these results. For one, there is a novelty factor at play. Whether one is pro-police or not, everyone knows who they are and understands what they do when they are engaged in traditional crime control. In contrast, the idea of public health officials suddenly tracking people, or police enforcing new and pervasive stay-at-home orders not related to traditional crime control efforts, is new to most people.

For another, the pandemic monitoring scenarios may imply a more universal form of surveillance than traditional law enforcement. Most often people think of traditional crime-fighting as directed at *people other than themselves*.[145] But when it comes to pandemic surveillance, everyone is a fair target. Prior work by several researchers has shown that privacy violations loom larger when they are directed at the self.[146]

On the question of universal surveillance, it is helpful to step back from the survey results and consider the one prior government program that looks like the kind of universal surveillance proposed here: the National Security Agency's phone-metadata program.[147] As with pandemic surveillance, this program collected personal information from almost the entire population. The NSA metadata program was conceived in the wake of the September 11th attacks and ran in one form or another until the 2015 passage of the USA FREEDOM Act fundamentally transformed it by imposing new restrictions.[148] Under the first instantiation of this program, the NSA appears to have been collecting the call records from every major telecom provider on a daily basis—effectively the call records of every American.[149] Though it did not collect the contents of those calls, it did know the numbers dialed and the call times and durations.[150] The intended use for this data was to look for patterns of calls between identified terrorism suspects and their unknown confederates.[151]

---

[145] *See, e.g.*, Susan J. Stabile, *Othering and the Law*, 12 U. ST. THOMAS L.J., 381, 395–96 (2016).

[146] *See, e.g.*, Chao, Durso, Farrell & Robertson, *supra* note 106, at 288, 299; Slobogin & Schumacher, *supra* note 20, at 759–60; Kugler & Strahilevitz, *supra* note 26, at 248 n.170.

[147] *See generally* Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. TIMES (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html [https://perma.cc/C68D-CU7Q].

[148] Obama v. Klayman, 800 F.3d 559, 561 (D.C. Cir. 2015) (describing the program and remanding to the district court to assess whether the litigation was moot following the passage of the USA FREEDOM Act).

[149] Klayman v. Obama, 957 F. Supp. 2d 1, 1, 7–8, 39 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015).

[150] *Id.* at 15–17.

[151] *Id.* at 15.

The NSA program attracted two conflicting judicial opinions on the issue of universal targeting. In one of these, *In re Application of the FBI*, the court ruled that the program was constitutionally permissible.[152] Broadly speaking, Judge Claire Eagan held that the collection of metadata was not generally a Fourth Amendment search, and that the aggregation of many actions, none of which were independently Fourth Amendment searches, did not suddenly create a Fourth Amendment search.[153]

Judge Richard Leon came to the opposite conclusion in *Klayman v. Obama*.[154] Relying on the concurrences in *Jones* that spoke about the importance of search duration, Leon concluded that aggregation did matter.[155] This mass surveillance was "almost-Orwellian" and not like anything that could have been "conceived" at the time of the 1979 *Smith* case, which held that metadata collection was not a search.[156] Simply put, the quantity mattered.[157]

Pandemic surveillance employing cellular location history is more intrusive than surveillance employing call history. In *Carpenter*, the Supreme Court has told us that cell phones are special, that they are necessities of modern life, and that even well-established Supreme Court doctrines must fall rather than be used to extinguish cell phone location privacy.[158] So, there

---

[152] *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *1 (FISA Ct. Aug. 29, 2013).

[153] *Id.* at *2 ("Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.").

[154] *See* 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015), *mooted by statute*, USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268. During the litigation, many judges expressed views of the merits. Now-Supreme Court Justice Brett Kavanaugh, for instance, agreed with the District Court in *In re Application of the FBI*. In a concurring opinion later in the *Klayman* litigation, he explained that he believed that the metadata program was constitutionally reasonable either because the collection of metadata was not a search under *Smith*, or because it was a reasonable special needs search. Klayman v. Obama, 805 F.3d 1148, 1149 (D.C. Cir. 2015) (Kavanaugh, J., concurring in a denial of rehearing en banc). But the shifting policies underlying the program prevented clear precedent on the pre-FREEDOM Act version.

[155] *See Klayman*, 957 F. Supp. 2d at 31–32 (citing United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring); *Jones*, 565 U.S. at 429–31 (Alito, J., concurring).

[156] *Klayman*, 957 F.Supp 2d at 33. (The pen register in *Smith* "in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its Bulk Telephony Metadata Program. It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.").

[157] *See id.* at 35–36.

[158] *See supra* notes 28–34.

is a clear Fourth Amendment interest at stake in pandemic surveillance, which relies heavily on cell phone contact tracing, even before turning to the issues of universal targeting.

The question for pandemic surveillance is whether the scale of the surveillance makes the existing Fourth Amendment problem exponentially worse. And, on that point, the argument presented in *Klayman* has strengthened over the years. In *Riley*, Chief Justice Roberts granted extra protection to electronic devices because there was "a quantitative and a qualitative" difference between them and the physical objects described in previous cases such as wallets and address books.[159] As in *Klayman*, quantity mattered.[160]

B. MAKING PANDEMIC SURVEILLANCE REASONABLE

That pandemic surveillance is seen as so intrusive and uses universal targeting counts against its reasonableness as a constitutional matter. This section begins by discussing the utility of pandemic surveillance and concludes by recommending safeguards that would make it reasonable.

As the COVID-19 pandemic progressed, countries took different approaches to contact tracing. Foreign governments in China, Taiwan, and elsewhere began using smartphone applications to do digital contact tracing.[161] In Asia, and, for a time, Israel, the approach to contact tracing was centralized and mandatory, while in much of Europe, countries favored a de-centralized approach premised on voluntary opting-in.[162] The centralized Israeli system was run through the domestic security agency.[163] When provided with the cellular number of an infected person, the agency was able to run that target number through its database of cellular information—message metadata, location information, tower connections—to seek out anyone who may have been within six feet of the target person for more than fifteen minutes within the preceding two weeks.[164] There was no enrollment

---

[159] Riley v. California, 573 U.S. 373, 391–93 (2014).

[160] *Id.*

[161] I. Glenn Cohen, Lawrence O. Gostin & Daniel J. Weitzner, *Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension*, 323 J. AM. MED. ASSOC. 2371, 2371–72 (2020).

[162] *Id.*

[163] Tehilla Shwartz Altshuler & Rachel Aridor Hershkowitz, *How Israel's COVID-19 Mass Surveillance Operation Works*, BROOKINGS (July 6, 2020), https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/ [https://perma.cc/BM8N-EN88].

[164] *Id.*

process; the government collected the information directly from various providers.[165]

The Apple and Google framework underlying the European systems, by contrast, allows people to install apps that cause each person's phone to broadcast an anonymized ID over Bluetooth.[166] This allows for other phones carrying the apps to record these IDs, creating a local record of contacts. When a person reports to the app that they have been diagnosed with COVID-19, the app allows a centralized server—which does not know who matches with what ID—to flag that person's ID, letting everyone else's app check whether that ID matches one of their contacts.[167] One substantial problem with this approach is persuading people to even install the application; uptake was fairly low in most countries.[168] In contrast with both these approaches, the United States has generally relied on manual contact tracing, the same technique used for prior diseases such as tuberculosis and HIV, with only scattered attempts to use decentralized digital technologies.[169]

Even with over 600,000 COVID-19-related deaths in the U.S.,[170] the list of unanswered questions about the disease remains long. It is still not clear how well digital contact tracing works.[171] At the beginning of a pandemic, when digital contact tracing might be most useful as the number of cases will be low,[172] less will be known. The case of Israel is a useful example on this point. At the start of the COVID-19 pandemic, the country's domestic intelligence agency was coordinating digital contact tracing with the aid of counterterrorism technology.[173] In retrospect, there are concerns regarding

---

[165] *Id.*

[166] *See* Kissick, Setzer & Schulz, *supra* note 5; Andy Greenberg, *How Apple and Google Are Enabling Covid-19 Contact-Tracing*, WIRED (Apr. 10, 2020, 3:37 PM), https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/ [https://perma.cc/ER3P-3FX5].

[167] *See* Greenberg, *supra* note 166.

[168] *See, e.g.*, Kissick, Setzer & Schulz, *supra* note 5.

[169] *See* Kissick, Setzer & Schulz, *supra* note 5; Cohen, Gostin & Weitzner, *supra* note 161.

[170] *Coronavirus in the U.S.: Latest Map and Case Count*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html [https://perma.cc/YR99-P76E] (last visited July 28, 2021).

[171] *See, e.g.*, Kissick, Setzer & Schulz, *supra* note 5.

[172] *See* Evan Anderson & Scott Burris, *Is Law Working? A Brief Look at the Legal Epidemiology of COVID-19*, *in* ASSESSING LEGAL RESPONSES TO COVID-19 20, 23 (Scott Burris, Sarah de Guia, Lance Gable, Donna E. Levin, Wendy E. Parmet & Nicholas P. Terry eds., 2020) (describing how early adoption of risk mitigation measures has substantial effect).

[173] Daniel Estrin, *Israel's Government Wants Spy Agency to Resume COVID-19 Tracing. Spy Chief Objects*, NPR (June 24, 2020, 1:17 PM), https://www.npr.org/sections/coronavirus-

the program's effectiveness: Israel's digital contact tracing technology identified less than 30% of positive COVID-19 cases, which could be due to the fact that "the technology is less effective at tracking subjects indoors."[174] But they did not know that then, and could not have. And time matters. Speed was a key factor in favor of South Korea's ability to contain the spread of COVID-19, for example.[175] How then should courts weigh immediate state needs against privacy risks given that information will often be lacking?

Initially, courts will largely have to defer to government experts on the question of whether the program will work. But the effectiveness of a surveillance program—the social value of allowing it—is only one side of the balancing test. The other side is the privacy cost, and that is much easier to assess, and limit, *ex ante*. That is why safeguards are so critical in this domain.

Many safeguards can be built *ex ante*, and they can be constantly refined as more information becomes available. We therefore believe that the reasonableness of a pandemic surveillance program is more a function of the safeguards it employs than any other factor. With this in mind, we propose the following restrictions for any government-led cell phone location surveillance programs during a public health emergency:

- Clearly identify who will have access to what data.
- Restrict law enforcement's access to cell location data for the purposes of criminal investigations.
- Restrict researchers' access to cell location data to only highly limited and narrow uses since location data is nearly impossible to fully anonymize.[176]
- Implement and enforce a staggered deletion system for cell location data, whereby health officials would be required to delete all identifiable data except for data corresponding to the most recent month.
- Engage in a continual review process assessing the necessity of the program. Since it is unlikely that a disease, such as COVID-19, will

live-updates/2020/06/24/882741912/israels-government-wants-spy-agency-to-resume-covid-19-tracing-spy-chief-objects [https://perma.cc/T4HR-EFDL].

[174] *Id.*

[175] *See Coronavirus: Fauci Warns of 100,000 US Cases Per Day*, BBC (June 30, 2020), https://www.bbc.com/news/world-us-canada-53237824 [https://perma.cc/9WLB-SUQW].

[176] *See, e.g.*, Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/Q35E-9FZB] (using anonymous location data to track and identify a Microsoft employee as he interviewed with and then started at a job Amazon). The fundamental problem is that very few people sleep in your house and work at your job.

ever fully be eradicated, government should have a clear goal, based on updated models as data becomes available, for when a digital surveillance system should be discontinued.

- Establish an audit system that ensures all data is deleted after it has been determined that the pandemic crisis has passed.

Efforts to implement privacy safeguards for large-scale public data collection are not new. Such programs often have sizable benefits, but also real privacy costs. For example, household energy usage data can be extremely useful for utilities for providing more efficient and cost-saving services, as well for consumers to engage in more climate-friendly behaviors.[177] Without proper safeguards, however, such data could easily be misused at the expense of one's right to privacy in the home.[178] As private tech companies such as Google and Apple have sought to enter the digital contact tracing game during COVID-19, they have built privacy protections into their applications, including opt-in and anonymization features, from the get-go.[179]

Fears of underregulated pandemic surveillance have already played out overseas. While South Korea has been hailed for its success in quickly containing the spread of the COVID-19 virus, in part due to the use of contact tracing technology, the country's government is facing criticism for what some see as a failure to protect individual privacy. Despite what the public had been told, it recently came to light that South Korea has been keeping patient information from a 2015 coronavirus outbreak, prompting concerns that it will not delete COVID-19 patient information as promised.[180]

The U.S. response to contact tracing, digital or otherwise, has been uncoordinated and ineffective. As of the summer of 2020, there is no federal approach to contact tracing, and state efforts have had mixed results.[181] On the analog-tracing side, response rates have been low. In New York City, which at the onset of the COVID-19 outbreak had one of the highest infection rates, the city's contact tracing response rate has been a mere 35% when it needed to be at least 75%.[182] Other states similarly using phone calls and

---

[177] *See* Kugler & Hurley, *supra* note 20, at 460–69.

[178] *Id.* at 453–54.

[179] *See* Cohen, Gostin & Weitzner, *supra* note 161, at 2371.

[180] Anthony Kuhn, *South Korea Holds onto Patient Data from Prior Coronavirus, Worrying Privacy Groups*, NPR (June 30, 2020, 11:00 AM), https://www.npr.org/sections/coronavirus-live-updates/2020/06/30/884580723/south-korea-holds-onto-patient-data-from-prior-coronavirus-worrying-privacy-grou [https://perma.cc/YF3Y-Y2NN].

[181] *See* Cohen, Gostin & Weitzner, *supra* note 161, at 2372.

[182] 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 [https://perma.cc/5T9K-FGFN].

survey questions for contact tracing—such as Massachusetts and Louisiana—have also had low response rates.[183]

And digital contact tracing, used by some states like North and South Dakota, has already led to real privacy problems.[184] Although the application maker had promised to make user information, including location data, private except to the states' Department of Health, in fact it shared some of that data with an outside marketing company.[185] In a small county in Texas, a government official improperly disclosed the names and addresses of COVID-positive patients with emergency personnel via text rather than through a secure, encrypted email, as required by local health officials.[186] Adding to these Texas residents' privacy concerns, even though lists with contact information for COVID-19 patients are in theory not supposed to be disseminated to an entire emergency department, such as police, in practice, they often are.[187]

The anti-COVID-19 lockdown and pro-BLM protests in May and June of 2020 further highlight the dangers of pandemic surveillance. State officials could easily use surveillance programs, particularly those designed to enforce stay-at-home orders, as pretext for tracing an individual's movements and activities beyond the scope of what is warranted in a health crisis. This could easily impinge on freedom of association.[188] Our proposal that law enforcement be barred from using pandemic surveillance data for traditional law enforcement purposes would help mitigate fears that health surveillance data would be repurposed by police to target those engaged in political protesting.

Similar restrictions on law enforcement use have previously accompanied some government data collection efforts. The Seventh Circuit, for example, recently found the installation of intrusive smart meters by a public utility reasonable in part because the statute required law enforcement

---

[183] *Id.*

[184] Geoffrey A. Fowler, *One of the First Contact-Tracing Apps Violates Its Own Privacy Policy*, WASH. POST (May 21, 2020), https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/ [https://perma.cc/DZ47-X7X8].

[185] *Id.*

[186] Telephone Interview with public health official in Texas (July 23, 2020) (on file with the Journal of Criminal Law and Criminology).

[187] *Id.*

[188] *See, e.g.*, NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460–66 (1958) (discussing how disclosure of an organization's membership list impinges on freedom of association); *see also* Ana Pajar Blinder, *Don't (Tower) Dump on Freedom of Association: Protest Surveillance under the First and Fourth Amendments*, 112 J. CRIM. L. & CRIMINOLOGY 125, 128-30, 133-137 (2021) (discussing how even the limited collection of location data can reveal politically meaningful associations and potentially chill freedom of expression).

to get a warrant to access the data.[189] The New Jersey Supreme Court's approval of nonconsensual HIV testing for certain sex offenders was likewise in part because the results of the test would not be shared with law enforcement.[190]

The safeguards we propose would have the effect of ensuring that any surveillance systems will incorporate privacy concerns into their design from the outset, before deployment. Our suggestions are consistent with the regulations approved in the existing case law on special needs searches and the related domain of constitutional protection for information privacy. On the Fourth Amendment front, consider *Naperville Smart Meter Awareness v. City of Naperville*.[191] In that case, the Seventh Circuit considered whether the city's installation of electricity smart meters, and the subsequent relaying of utility information, amounted to an unreasonably invasive government search.[192] In finding that the collection of home utility data was reasonable, the court emphasized that, despite the substantial privacy intrusion into the home, the data collection was tailored to the limited, non-law enforcement purpose identified by the government and could not be shared or repurposed in a manner inconsistent with that purpose.[193]

The Supreme Court also considered safeguards to be highly important in the constitutional information privacy case *Whalen v. Roe*.[194] As one of the few Supreme Court cases that directly addresses health information privacy concerns, *Whalen* is key for considering constitutional safeguards. *Whalen* came at a time when the government was concerned with a different type of public health crisis: growing prescription drug abuse.[195] At issue was whether the prescription reporting requirement of a New York statute aimed at curbing illicit drug use was unreasonably intrusive.[196] The Court did not believe the program posed a sufficiently grievous threat to constitutional privacy interests where the state interest—"to minimize the misuse of

---

[189] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018) ("And Naperville's amended 'Smart Grid Customer Bill of Rights' clarifies that the city's public utility will not provide customer data to third parties, including law enforcement, without a warrant or court order.").

[190] *In re* J.G., 701 A.2d 1260, 1262, 1266–67 (1997) (results would be shared with the complaining victim and victim support services but could not be used for prosecution or shared with the prosecutor's office).

[191] 900 F.3d 521 (7th Cir. 2018).

[192] *Id.* at 528.

[193] *Id.* at 528–29.

[194] 429 U.S. 589 at 593–95 (1977).

[195] *See id.* at 591–92.

[196] *Id.* at 591–96.

dangerous drugs"[197]—was great and the state had shown a good-faith effort to protect individual information.[198] In addressing patient concerns about misuse of the data, such as by law enforcement officials, the Court noted the extensive security provisions taken to guard patient data, including: strict limits on who had access to patient files,[199] a statutory requirement that patient records be destroyed after five years, a "locked wire fence" surrounding the room where the vault with the records was kept, an alarm system, use of a locked cabinet to guard the computer tapes, and the "off-line" feature used to run the computer files.[200] In addition to these extensive safeguards, the Court noted there was little reason to believe the information would be misused: the New York statute governing this information collection system included a nondisclosure provision which made "[w]illful violation . . . a crime punishable by up to one year in prison and a $2,000 fine,"[201] making it unlikely, by the Court's reasoning, that such a provision would be violated.[202]

What does this mean for states attempting to collect individual health information during the COVID-19 crisis? *Whalen* shows how the incorporation of robust privacy safeguards can justifiably lead to judicial deference to government officials during a public health crisis. Despite the drug crisis of the 1970s, the Court did not give the government free rein to do with patient information as it pleased, but instead looked to whether and how the government was protecting patient privacy.[203] First, the Court was able to pinpoint evidence of existing privacy safeguards, including internal controls as well as external restrictions in the form of statutory sanctions.[204] In the COVID-19 context, many states have undertaken contact tracing even as legislation about safeguards failed to advance at the federal level.[205] Second, the state interest in *Whalen* was curbing prescriptions for drugs with

---

[197] *Id.* at 598.

[198] *Id.* at 597–98.

[199] *Id.* at 595 (noting that only seventeen Department of Health officials had access to the files).

[200] *Id.* at 593–94.

[201] *Id.* at 594–95.

[202] *See id.* at 601 n.27.

[203] *Id.* at 597–98.

[204] *Id.* at 593–95.

[205] Jessica Rich, *How Our Outdated Privacy Laws Doomed Contact-Tracing Apps*, BROOKINGS (Jan. 28, 2021), https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/ [https://perma.cc/4CUM-J2TP].

a high potential for abuse, which targets only those in the population who take such drugs.[206] Contact tracing programs target the entire population.[207]

Although the *Whalen* Court approved of the New York program, it emphasized that its opinion did not reach any questions related to unlawful disclosure of private information or to data collection by systems "that did not contain comparable security provisions."[208] This should be taken as a warning note for those interested in pandemic surveillance. A digital contact tracing program could easily be constitutional, given appropriate safeguards. Without such safeguards, the extreme intrusiveness of a digital surveillance program likely runs afoul of the Constitution.

C. SAFEGUARDS AND PUBLIC TRUST

In addition to helping a pandemic surveillance program pass constitutional muster, the implementation of safeguards might also work to build public trust in the program. As our data show, distrust of public health officials is related to viewing pandemic surveillance as more intrusive. And more people expressed skepticism about the effectiveness of the monitoring than thought it would help control the spread of the infection.[209] This is consistent with other work from April 2020 that similarly found skepticism in the efficacy of contact tracing, with 60% of respondents saying that government contact tracing would "not make much of a difference in limiting the spread" of COVID-19.[210]

Other studies have also shown that Americans have, at best, mixed views of deferring to public health experts on tracking. One survey study from Spring 2020 found that about 60% of Americans would be willing to voluntarily install a contact tracing application on their phones to mitigate the spread of COVID-19, but only about one third said that they would use such an application were it provided by a public health agency.[211] Worse,

---

[206] *Whalen*, 429 U.S. at 598.

[207] *See* Altshuler & Hershkowitz, *supra* note 163 (describing how making contract tracing compulsory for all citizens was an effective way to manage the pandemic).

[208] *Whalen*, 429 U.S. at 605–06.

[209] *See supra* Section II.A.

[210] PEW RSCH. CTR., TOPLINE COVID & CELLPHONES (Apr. 7–12, 2020), https://www.pewresearch.org/wp-content/uploads/2020/04/Topline-COVID-cellphones.pdf [https://perma.cc/92ES-35XS]. Further, this study found that a slight majority was in favor of tracking those who have tested positive for COVID-19 using their phones (52% vs. 48%), but that stronger majorities were opposed to tracking those who might have had contact with them (55% vs. 45%) or using cell phone data to enforce social contact restrictions (63% vs. 37%).

[211] Eszter Hargittai & Elissa Redmiles, *Will American Be Willing to Install COVID-19 Tracking Apps?*, SCI. AM. (Apr. 28, 2020), https://blogs.scientificamerican.com/observations/will-americans-be-willing-to-install-covid-19-tracking-apps/ [https://perma.cc/T8LD-H67P].

other potential providers were not more popular; only about 20% would want a technology company provider and under 15% a public university.[212] Similarly, a study commissioned by CyberNews found that only 30% of people would allow a state sponsored app to display their location to other local residents if they contracted the virus.[213]

Collectively, these data show the problem of lacking a trusted data intermediary. Even among those who think a digital contact tracing program would be useful, there is no consensus about who should run it. Our data show that the public seems most concerned about such data being repurposed by governments or technology companies in a way that violates their privacy.[214] One way to gain public trust in health surveillance programs is to counteract that concern by having the government publicly and credibly commit to a limited program and establish procedures such that this promise can be kept.

Building in safeguards from the beginning will never guarantee the absence of privacy risk, but it can minimize potential costs of pandemic surveillance. A recent study by the authors shows that, to date, law enforcement has not taken on a significant role with regards to COVID-19, but that does not mean it could not or would not in the future.[215] The potential efficiencies of digital contact tracing and digital quarantine enforcement are large. Neither is occurring in the United States right now, but maybe they should be. That is a valid policy choice. But we should not forget the constitutional guarantee of reasonableness as we build these programs. Too easily one could create a regime where the tools of mass surveillance are being used to monitor anyone who leaves their home for purposes beyond public health, and to keep this surveillance going for years to come.

---

[212] *Id.*

[213] Edvardas Mikalauskas, *Coronavirus Survey: Among Americans, Support for Privacy Rights Trumps Fear of Pandemic*, CYBERNEWS, (Apr. 24, 2020), https://cybernews.com/privacy/report-among-americans-support-for-privacy-rights-trumps-fear-of-pandemic/ [https://perma.cc/KEH2-K3AZ]. The questions in this survey appear to have been somewhat biased. For example, one read "Would you approve the use of controversial practices by the authorities (such as using facial recognition and phone data collection) to fight the spread of the pandemic, even at the expense of your personal privacy?" This question is loaded, twice priming a pro-privacy response. *Id.*

[214] See the rationales people cite in *supra* Section II.A.

[215] Matthew B. Kugler, Mariana Oliver, Jonathan Chu & Nathan R. Lee, *American Law Enforcement Responses to COVID-19*, 111 J. CRIM. L. & CRIMINOLOGY ONLINE 19, 29–30 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3707087 [https://perma.cc/2W2A-BE6U].

CONCLUSION

Despite the depths of this crisis, Americans still perceived COVID-19 surveillance to be more intrusive than surveillance aimed at general crime control, and therefore worthy of greater regulation. At the very least, we should respond to these public privacy concerns by constructing safeguards that limit the uses of pandemic surveillance data and explaining to the public just how we plan to use these data during this new normal.

APPENDIX

Demographics of the samples

	April, 2020 N = 1,178		June, 2020 N = 1,197		Census[216]
% Female	51.6		50.5		50.8
% Male	48.0		49.3		49.2
% Other	.4		.3		
Age (years)					
Median	48		48		
Mean	47.24	(17.56)	47.46	(17.43)	
Political Orientation (1–7)[217]	4.08	(1.76)	4.00	(1.77)	
Race/Ethnicity (%)					
White	77.2		75.9		76.3
Black or AA	12.7		14.1		13.4
Indian or Native	.7		.8		1.3
SE Asian	5.9		5.9		5.9
Hawaiian/Pacific	.3		.3		.2
Multiracial or Other	3.1		3.0		2.8
Hispanic (%)	16.4		17.9		18.5
Education					
Less than HS	9.3		11.0		10.9
HS Diploma/GED	29.9		28.2		28.6
Two-Year College	28.7		28.4		28.2
Four-Year College	20.5		20.8		20.6
Graduate Degree	11.6		11.6		11.6

Notes: For age and political orientation, the numbers in parentheses represent standard deviations. Hispanic identity was assessed in a separate question.

[216] Ethnicity and gender statistics are from the Census.gov website. *Quick Facts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts//fact//table//US//PST045217 [https://perma.cc/HM2A-QBZC]. Educational attainment was calculated from data in *Educational Attainment in the United States: 2018*, U.S. CENSUS BUREAU (Feb. 21, 2019), https://www.census.gov/data/tables/2018/demo/education-attainment/cps-detailed-tables.html [https://perma.cc/XJ3N-AQDZ]. Note that the demographic numbers do not sum to 100% due to rounding.

[217] Political orientation was assessed on a scale ranging from 1-Very Liberal to 7-Very Conservative.

Table 1A: Wave 1 intrusiveness of different searches depending on search context

	Police investigation	Public Health/ Pandemic	Police/ Stay-at-home
Cell phone location data tracking a phone's movements (month)	58.77_{a} (31.94)	74.41_{b} (28.61)	72.25_{b} (28.99)
Cell phone records of who was at a particular location at a particular time	63.04_{a} (31.24)	70.52_{b} (28.60)	70.55_{b} (28.89)
Cell phone location data to trace whose phones were near a certain person (day)	63.42_{a} (30.00)	72.22_{b} (28.30)	71.56_{b} (28.86)
Credit card charges from CC company to track movements (month)	60.75_{a} (32.00)	78.08_{b} (26.46)	74.37_{b} (28.82)
Use facial recognition to match images of people in public park	50.13_{a} (33.34)	67.01_{c} (31.32)	59.52_{b} (33.90)
Power usage data from utility to see if consistent with person at home	59.11_{a} (32.88)	69.21_{b} (30.39)	70.76_{b} (29.74)
Drone recording video of people who are outside	58.23_{a} (33.12)	64.67_{b} (33.14)	59.45_{ab} (32.51)

Notes: Means not sharing subscripts differ significantly at the $p < .05$ level. Numbers in parentheses are standard deviations.

Table 2A: Wave 2 intrusiveness of different searches depending on search context

	Police investigation	Public Health/ Pandemic	Police/ Stay-at-home
Cell phone location data tracking a phone's movements (month)	56.32_a	72.50_b	73.31_b
	(31.97)	(28.07)	(27.47)
Cell phone records of who was at a particular location at a particular time	58.78_a	68.34_b	70.01_b
	(31.75)	(29.36)	(29.01)
Cell phone location data to trace whose phones were near a certain person (day)	60.07_a	68.79_b	71.24_b
	(31.97)	(28.81)	(28.61)
Credit card charges from CC company to track movements (month)	57.51_a	76.67_b	76.85_b
	(32.14)	(26.98)	(26.74)
Use facial recognition to match images of people in public park	50.54_a	66.82_b	63.99_b
	(32.68)	(29.54)	(31.07)
Power usage data from utility to see if consistent with person at home	55.95_a	70.45_b	70.95_b
	(32.85)	(28.57)	(29.85)
Drone recording video of people who are outside	55.05_a	67.25_b	63.63_b
	(32.68)	(30.47)	(31.36)

Notes: Means not sharing subscripts differ significantly at the $p < .05$ level. Numbers in parentheses are standard deviations.

Table 3A: Wave 2 reasonable expectations of privacy of different searches depending on search context

	Police investigation	Public Health/ Pandemic	Police/ Stay-at-home
Cell phone location data tracking a phone's movements (month)	3.21_a (1.35)	3.84_b (1.26)	3.86_b (1.30)
Cell phone records of who was at a particular location at a particular time	3.30_a (1.38)	3.66_b (1.28)	3.71_b (1.30)
Cell phone location data to trace whose phones were near a certain person (day)	3.31_a (1.36)	3.74_b (1.24)	3.82_b (1.25)
Credit card charges from CC company to track movements (month)	3.15_a (1.39)	4.06_b (1.19)	3.94_b (1.32)
Use facial recognition to match images of people in public park	2.91_a (1.40)	3.64_b (1.30)	3.44_b (1.40)
Power usage data from utility to see if consistent with person at home	3.20_a (1.37)	3.82_b (1.26)	3.84_b (1.31)
Drone recording video of people who are outside	3.08_a (1.43)	3.64_b (1.34)	3.50_b (1.35)

Notes: Means not sharing subscripts differ significantly at the $p < .05$ level. Numbers in parentheses are standard deviations.

Table 4A: Wave 1 percentage of people believing a warrant or court order should be required

	Police investigation	Public Health/ Pandemic	Police/ Stay-at-home
Cell phone location data tracking a phone's movements (month)	66.3%	72.4%	79.0%
Cell phone records of who was at a particular location at a particular time	66.3%	70.6%	73.6%
Cell phone location data to trace whose phones were near a certain person (day)	67.4%	68.8%	76.3%
Credit card charges from CC company to track movements (month)	69.7%	77.1%	80.5%
Use facial recognition to match images of people in public park	43.2%	63.8%	55.8%
Power usage data from utility to see if consistent with person at home	65.0%	70.6%	74.8%
Drone recording video of people who are outside	56.8%	58.3%	55.6%

Table 5A: Percentage of people above and below the midpoint on the reasonable expectation of privacy scale by condition

	Law Enforcement		Public Health		Law Enforcement Stay-at-Home	
	Below	Above	Below	Above	Below	Above
Cell phone location data tracking a phone's movements (month)	31.9%	43.5%	15.2%	66.0%	15.0%	65.3%
Cell phone records of who was at a particular location at a particular time	26.2%	48.0%	17.9%	59.1%	18.0%	59.8%
Cell phone location data to trace whose phones were near a certain person (day)	26.2%	47.0%	16.0%	62.2%	15.8%	63.2%
Credit card charges from CC company to track movements (month)	32.2%	43.8%	11.9%	71.8%	14.5%	68.1%
Use facial recognition to match images of people in public park	41.7%	33.0%	20.0%	55.3%	26.8%	49.3%
Power usage data from utility to see if consistent with person at home	30.5%	44.9%	16.6%	61.3%	17.5%	63.5%
Drone recording video of people who are outside	32.5%	4.04%	23.8%	55.5%	24.7%	49.1%

Notes: Participants were asked to rate whether the search "violated a reasonable expectation of privacy" on a scale ranging from Definitely Not (1) – Definitely Yes (5). Responses above the midpoint (3) indicate agreement with the notion that privacy was violated. Responses below the midpoint indicate disagreement.