THE CITY UNIVERSITY OF NEW YORK LAW REVIEW

City University of New York Law Review

Volume 24 | Issue 1

Winter 2021

How the Fallout from Post-9/11 Surveillance Programs Can Inform Privacy Protections for COVID-19 Contact Tracing Programs

Emma Mendelson
CUNY School of Law

HOW THE FALLOUT FROM POST-9/11 SURVEILLANCE PROGRAMS CAN INFORM PRIVACY PROTECTIONS FOR COVID-19 CONTACT TRACING PROGRAMS

Emma Mendelson†

INTRODUCTION

In times of national crisis, the government often endows itself with broad and unprecedented powers.[1] Following the events on September 11, 2001, the United States government enhanced the scope of its surveillance capabilities in the name of preventing terrorist activity; privacy was second to alleged safety as Congress reacted rashly to pass legislation.[2] As the United States responds to the global crisis of COVID-19, surveillance

† Emma Mendelson is a part-time 3L at CUNY School of Law.

[1] *See, e.g.*, Alex Joel, *9/11 All Over Again*, JUST SECURITY (Apr. 10, 2020), https://perma.cc/7YUL-X88P; Emergency Banking Relief Act, Pub. L. No. 73-1, 48 Stat. 1 (1933); War Powers Act of 1941, Pub. L. No. 77-354, 55 Stat. 838.

[2] Peter Swire, *Security, Privacy and the Coronavirus: Lessons from 9/11*, LAWFARE (Mar. 24, 2020, 2:46 PM), https://perma.cc/93RB-LWTP.

has returned as an integral tool for national security: Both local and federal governments are using location metadata and health data to assist in preventing the disease's spread.[3]

"Contact [or proximity] tracing—which involves figuring out who an infected person has been in contact with and trying to prevent them from infecting others—is one of the most promising solutions" for monitoring COVID-19 and has manifested through government contracts with private technology providers like Google and Apple.[4] These private, third-party corporations collect not only content-based data (e.g., e-mails and direct messages) from their users, but also metadata, such as user location, which is continuously and passively uploaded into each of the companies' servers.[5] While content-based data have been given certain legal protections,[6] the government's acquisition of metadata from private, third parties is still open to interpretation.[7]

During the response to the COVID-19 pandemic, there has been a key shift in the "expected" surveilled population[8] from the post-9/11 era.

---

[3] *CDC COVID-19 Surveillance*, Subheading of *FAQ: COVID-19 Data and Surveillance*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://perma.cc/L5YC-N3P8 (last updated Nov. 20, 2020); *COVIDView Weekly Summary*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://perma.cc/E74F-WHBF (last updated Sept. 28, 2020); Benjamin Lesser et al., *Special Report: Local Governments 'Overwhelmed' in Race to Trace U.S. COVID Contacts*, REUTERS (Aug. 4, 2020, 7:16 AM), https://www.reuters.com/article/us-health-coronavirus-tracing-specialrep/special-report-local-governments-overwhelmed-in-race-to-trace-u-s-covid-contacts-idUSKCN2501GK.

[4] Russell Brandom & Adi Robertson, *Apple and Google Are Building a Coronavirus Tracking System into iOS and Android*, VERGE (Apr. 10, 2020, 12:58 PM), https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app.

[5] During oral argument for *Carpenter v. United States*, Supreme Court Justice Sonia Sotomayor commented on the dangers of unprotected metadata collection. When a cell phone becomes "an appendage" for the individual (e.g., where people sleep with the phone in their bed), the collection of contentless metadata in the aggregate, which includes location data, reveals a substantial amount of information, comparable to the collection of content data. Transcript of Oral Argument at 42-43, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402); *see also* Amy Davidson Sorkin, *In* Carpenter *Case, Justice Sotomayor Tries to Picture the Smartphone Future*, NEW YORKER (Nov. 30, 2017), https://perma.cc/RQ6P-PDHR.

[6] The Stored Communications Act (SCA) was enacted as part of the Electronic Communications Privacy Act (ECPA) in 1986. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701-13 (2018). By passing the ECPA, Congress closed the gaps in privacy protection for wire and electronic communications and transactional records because the Fourth Amendment's right to be "secure in [one's] persons, houses, papers, and effects, against unreasonable searches and seizures," did not include electronic communications. U.S. CONST. amend. IV.

[7] *See Carpenter*, 138 S. Ct. at 2210-11 (holding a warrant is required when police seek cell phone tower data in connection with alleged criminal activity from a third-party).

[8] "Expected" in this context means the population that was intended to be surveilled versus the one actually surveilled. For example, the USA PATRIOT Act was meant to "deter and

Rather than surveillance policy that is outwardly aimed at allegedly *suspect* populations (e.g., terrorists[9] or those affiliated with such), it can now include all U.S. citizens at home or abroad, non-citizens in the country, and others trying to enter the country. The current volume of users presents an unprecedented surveillance landscape. As of August 10, 2020, Facebook had over 2.7 billion monthly active users.[10] As of April 30, 2020, Google Chrome, a cross-platform web browser that saves everything a user does (e.g., search history, email content, location) to their Google account, had over two billion users.[11] The prevalence of third-party data platforms without any meaningful change in third-party data laws has caused significant violations of individuals' right to privacy—and will continue to do so.[12]

---

punish terrorist acts in the United States and around the world" by intercepting communications from "non-United States persons." Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, pmbl., § 207, 115 Stat. 272 (2001) [hereinafter USA PATRIOT Act] (codified as amended in scattered sections of U.S.C.); *see also* Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, GUARDIAN (June 20, 2013, 6:59 PM), https://perma.cc/BA8A-9SSC. In practice, the USA PATRIOT Act was used to collect massive amounts of domestic communications from people with no connections to terrorist acts or groups. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013, 3:23 PM), https://perma.cc/SK93-NT6R.

[9] The author uses this term because it is the language of the post-9/11 surveillance laws being discussed. This language has enabled significant anti-Muslim hatred, is used to dehumanize individuals in the name of national security, and will only be used in this Note as necessary.

[10] J. Clement, *Facebook: Number of Monthly Active Users Worldwide 2008-2020*, STATISTA (Nov. 24, 2020), https://perma.cc/7UKQ-S4EH; *see also* Briana M. Trifiro & Jennifer Gerson, *Social Media Usage Patterns: Research Note Regarding the Lack of Universal Validated Measures for Active and Passive Use*, SOC. MEDIA & SOC'Y, Apr.-June 2019, at 1-2, https://perma.cc/9YWZ-K6ZT ("[A]ctive social media usage refers to online behaviors that facilitate 'direct exchanges' among users . . . . Active social use represents direct written communication between the user and their friends . . . .").

[11] Gordon Kelly, *Google Chrome Crash Reports Grow with New Error Reports*, FORBES (last updated Apr. 30, 2020, 7:27 AM), https://perma.cc/XMN6-YDEU (stating a Chrome software update was distributed on or around April 29, 2020, "to the browser's two billion users worldwide.").

[12] Since its passage in 1986, ECPA has not been amended to account for technological advances. *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, https://perma.cc/W87X-YHN4 ("Since 1986, technology has advanced at breakneck speed while electronic privacy law remained at a standstill."). Meanwhile, the SCA, Title II of the ECPA, was minimally amended in 2018 to incorporate modern technology, with the Clarifying Lawful Overseas Use of Data (CLOUD) Act. Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, §§ 101-06, 132 Stat. 348 (2018). The CLOUD Act allowed federal law enforcement to compel U.S.-based tech companies to turn over data, regardless of whether the data was stored domestically or abroad. Michael E. Lackey & Oral D. Pottinger,

Applying the lessons learned from post-9/11 surveillance laws and programs that created blanket searches of domestic communications in the name of national security[13] could be valuable as the United States traverses this thicketed terrain. This Note will identify key takeaways from the post-9/11 era and use them to contextualize surveillance practices during the COVID-19 pandemic. Part I discusses the post-9/11 legislation that broadened the government's surveillance powers. Part II examines how the Trump administration responded to the COVID-19 outbreak. Both Parts I and II consider the types of data being sought and the government agencies involved, along with the data collection methods employed. Finally, Part III suggests some protective courses of action by considering the fallout from the post-9/11 era of surveillance and its abuses of individual privacy rights. While data surveillance will be an integral tool in slowing the spread of COVID-19, the post-9/11 era has shown the kinds of egregious personal violations that occur when government surveillance programs are allowed to act in secrecy and given unfettered deference.[14]

I. THE BUSH ADMINISTRATION AND THE BROADENED SCOPE OF SURVEILLANCE

A. The Law and the NSA

The Foreign Intelligence Surveillance Act of 1978 (FISA)[15] is a good jumping-off point for a conversation about modern surveillance programs. FISA is an invention of the Cold War era and a response to extensive government surveillance that had been growing since the early 20th century, as new technologies created public insecurity over the government's reach into individuals' lives.[16] The Act provided the acceptable

Stored Communications Act: Practical Considerations, LEXISNEXIS (June 22, 2018), https://perma.cc/9EKG-WX9Z.

[13] *See, e.g.*, Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of U.S.C.); Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, Pub. L. No. 114-23, 129 Stat. 268; USA PATRIOT Act.

[14] Joseph Zeballos-Roig, *7 Ways that 9/11 Created a Dystopian Security Landscape that Americans Are Still Living in*, BUS. INSIDER (Sept. 11, 2019, 2:34 PM), https://perma.cc/4QMH-9KXY.

[15] Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of U.S.C.).

[16] For decades following World War II, "as part of its SHAMROCK [and MINARET] Program[s], the government collected and turned over to the NSA millions of telegrams that originated within, terminated in, or traveled through the United States." G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 869 (2003). This coincided with the Red Scare—"paranoia about the internal Communist threat"—following World War II because of fears over the Soviet Union's occupation of Eastern Europe.

means for physical and electronic surveillance (e.g., wiretapping, access to business records, pen registers), along with judicial and congressional oversight of intelligence agencies.[17]

But these regulations were loose. For instance, while judicial authorization was required to spy on non-U.S. persons for more than three days, spying could begin 72 hours *before* authorization was given.[18] Moreover, the Foreign Intelligence Surveillance Court (FISC), the court created under FISA, has a reputation of deferring to the National Security Agency's (NSA) judgment without much scrutiny.[19] The court was also designed to maintain secrecy for the sake of national security, offering little in the way of accountability.[20] FISC has no obligation to reveal court documents or decisions about the warrants it approves.[21]

Initially, counter-terrorist initiatives following 9/11 were bipartisan, helping legislation move quickly.[22] Much of that support resulted from the Bush administration harassing Congress with threats of potential future attacks.[23] Attorney General John Ashcroft's office began drafting legislation to provide "access to [previously unavailable] legal tools in order to more effectively combat terrorism."[24] These efforts culminated

---

McCarthyism and the Red Scare, U. VA. MILLER CTR., https://perma.cc/H9HP-EFVK (last visited Aug. 29, 2020). Domestic espionage projects like MINARET and SHAMROCK were driven by anti-communist sentiment from the White House and aimed at prominent figures, such as Muhammad Ali and Martin Luther King, Jr., who were protesting the Vietnam War. Matthew M. Aid & William Burr, *Secret Cold War Documents Reveal NSA Spied on Senators*, FOREIGN POL'Y (Sept. 25, 2013, 8:30 PM), https://perma.cc/H6MY-WG9X.

[17] Foreign Intelligence Surveillance Act of 1978 §§ 102-03, 108.

[18] 50 U.S.C. § 1805(f)(1) (2020).

[19] Between 1979 and 2012, "the court overseeing the Foreign Intelligence Surveillance Act has rejected only 11 of the more than 33,900 surveillance applications by the government, according to annual Justice Department reports to Congress." Evan Perez, *Secret Court's Oversight Gets Scrutiny*, WALL ST. J. (June 9, 2013, 7:11 PM), https://perma.cc/48AH-NZQD.

[20] *5-4: Clapper v. Amnesty International*, WESTWOOD ONE PODCAST NETWORK (May 12, 2020) (downloaded using Stitcher).

[21] *Id.*

[22] The 9/11 Commission was a bipartisan collection of lawmakers who probed into 9/11, identified what kinds of "mistakes could be prevented in the future," and created the *9/11 Commission Report*. Sam Brodey, *A Bipartisan Commission Came Together After 9/11. Don't Count on It for COVID-19.*, DAILY BEAST (Apr. 8, 2020, 6:56 AM), https://perma.cc/2D99-2BMK; *see also* Dara Lind, *Everyone's Heard of the Patriot Act. Here's What It Actually Does.*, VOX (June 2, 2015, 8:30 AM), https://www.vox.com/2015/6/2/8701499/patriot-act-explain; Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 951-52 (2006).

[23] *See generally Surveillance Under the USA/Patriot Act*, ACLU, https://perma.cc/FRH9-XKDN (last visited Dec. 29, 2020).

[24] Joshua H. Pike, *The Impact of a Knee-Jerk Reaction: The Patriot Act Amendments to the Foreign Intelligence Surveillance Act and the Ability of One Word to Erase Established Constitutional Requirements*, 36 HOFSTRA L. REV. 185, 211 (2007) (citing JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 154 (2006)). "[S]uch legal tools

in the USA PATRIOT Act, signed into law by George W. Bush on October 26, 2001, about a month and a half after 9/11.[25] Since its enactment, not only has the USA PATRIOT Act become synonymous with broad governmental powers of surveillance, it also expanded other executive powers, like detention powers and the authority to generate funding for counter-terrorism.[26] Some key, surveillance-specific provisions of the USA PATRIOT Act are[27]: section 215 (third-party records searches);[28] section 213 (private property searches without owner's notice);[29] section 218 (expanding the Fourth Amendment's exception to collection of foreign intelligence information);[30] section 214 (surveilling "foreign intelligence information not concerning a United States person");[31] and the National Security Letters Provision ("expand[ing] the FBI's authority to demand personal customer records from Internet Service Providers . . . without prior court approval").[32] Section 215—along with the rarely-used sections 206[33] and 207[34]—were temporary provisions that were set to (and did) sunset in 2015.[35]

FISA was amended by the USA PATRIOT Act under Title II, Section 218.[36] Originally, FISA contained an exception to the Fourth Amendment's probable cause requirement: Wiretapping or general searches

included amending the legal standard for acquiring a FISA order and the degree of permissible communications between criminal prosecutors and foreign intelligence agents." *Id.* at 210 n.126 (citing ASHCROFT, *supra*, at 156).

[25] *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[26] *See* Lind, *supra* note 22.

[27] For summaries of the following sections, see *Surveillance Under the USA/Patriot Act*, *supra* note 23.

[28] USA PATRIOT Act § 215. Section 215 sunsetted on March 15, 2020. India McKinney, *Section 215 Expired: Year in Review 2020*, ELEC. FRONTIER FOUND. (Dec. 29, 2020), https://perma.cc/ZYE2-YYCH.

[29] USA PATRIOT Act § 213.

[30] *Id.* § 218.

[31] *Id.* § 214.

[32] *National Security Letters*, ACLU, https://perma.cc/U96D-FL36 (last visited Dec. 29, 2020).

[33] The "roving wiretap" provision is where a wiretap follows an individual. *See* USA PATRIOT Act § 206.

[34] The "lone wolf" provision is where the government has "probable cause" to surveil a target but cannot show the target's link to a foreign terrorist organization or foreign power. USA PATRIOT Act § 207; *see also* 50 U.S.C. § 1801(b)(1)(C); Robert Chesney, *Why Is the Lone Wolf FISA Provision Never Used? And Just How Broad Is the FISC Understanding of Group Agency?*, LAWFARE (June 3, 2015, 2:13 PM), https://perma.cc/BKA9-PKPY.

[35] Lind, *supra* note 22; McKinney, *supra* note 28.

[36] USA PATRIOT Act § 218.

could occur "only if the *primary purpose* was to gather foreign intelligence."[37] Section 218 changed the "primary purpose" requirement of foreign intelligence-gathering to a "significant purpose" requirement, loosening the evidentiary standard.[38] Changing to the "significant purpose" standard allowed the government to "circumvent the traditional warrant requirements of the Fourth Amendment,"[39] even if the primary purpose was to gather criminal evidence.[40]

Before FISA and the USA PATRIOT Act, the NSA, a government intelligence agency, engaged in domestic surveillance for decades.[41] The NSA had projects like SHAMROCK that intercepted telegraphic data (e.g., telegrams) entering and exiting the United States.[42] Its sister project, MINARET, involved intercepting domestic electronic communications and transmitting them to other federal intelligence agencies, like the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA).[43] ThinThread, designed by William Binney, Ed Loomis, and J. Kirk Wiebe,[44] was a program from the 1990s that enhanced wiretapping by providing the architecture to analyze the vast amount of data the NSA was collecting and then dump irrelevant data to comply with Fourth Amendment warrantless search and seizure rights.[45] Three weeks prior to 9/11, ThinThread was sidelined by Trailblazer, an essentially identical,

---

[37] *Surveillance Under the USA/Patriot Act*, *supra* note 23 (emphasis added).

[38] Pike, *supra* note 24 ("Section 218 . . . amended 50 U.S.C. § 1804(a)(7)(B) of FISA to require the significant purpose of a FISA order be for foreign intelligence, rather than the previously required primary purpose or purpose requirement."); Jennifer L. Sullivan, *From the Purpose to a Significant Purpose: Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 379, 381 (2005) ("While authorization for a FISA court order traditionally entailed certification that 'the purpose' of the surveillance was to acquire foreign intelligence, section 218 allows the FISA court to issue a FISA warrant if 'a significant purpose' of the investigation is foreign intelligence surveillance.") (footnotes omitted).

[39] Sullivan, *supra* note 38, at 412.

[40] Pike, *supra* note 24.

[41] *NSA Timeline 1791-2015*, ELEC. FRONTIER FOUND., https://perma.cc/QKS8-548G.

[42] S. REP. NO. 94-755, at 765 (1976).

[43] *See* Lisa Graves, *The Right to Privacy in Light of Presidents' Programs: What Project MINARET's Admissions Reveal About Modern Surveillance of Americans*, 88 TEX. L. REV. 1855, 1879-80 (2010).

[44] *ThinThread Whistleblowers*, GOV'T ACCOUNTABILITY PROJECT (May 7, 2020), https://perma.cc/5EQZ-VUKA.

[45] Patrick G. Eddington, *Hayden, NSA, and the Road to 9/11*, JUST SECURITY (Dec. 7, 2017), https://perma.cc/7W6K-8XJ3.

though exorbitantly more flawed, project[46] that, notably, lacked Fourth Amendment protections.[47]

After 9/11 and the USA PATRIOT Act's enactment—and following an executive order from George W. Bush[48]—the NSA implemented the Terrorist Surveillance Program, which enabled the comprehensive, warrantless seizure of electronic data (e.g., interception of phone conversations and private e-mails).[49] Oversight was more relaxed under the Terrorist Surveillance Program than it had been under FISA. Rather than limit surveillance target decision-making to senior staff members, under the Terrorist Surveillance Program "targets . . . may be chosen by the 'operational work force' at the NSA and approved by a shift supervisor."[50] And while the Terrorist Surveillance Program ended in 2007, it paved the way for other programs like PRISM, OAKSTAR, and STORMBREW, which allowed the NSA—so long as it received FISC's blessing—to conduct dragnet searches of data from users of private internet service providers.[51] These programs were created under the Protect America Act of

---

[46] By the time it was abandoned in 2006, Trailblazer had cost the government $1.2 billion and "stalled at the level of schematic drawings . . . ." Jane Mayer, *The Secret Sharer*, NEW YORKER (May 23, 2011), https://perma.cc/BL3P-ZW63; *see also* Tim Shorrock, *Obama's Crackdown on Whistleblowers*, NATION (Mar. 26, 2013), https://www.thenation.com/article/archive/obamas-crackdown-whistleblowers/; Eddington, *supra* note 45.

[47] Rather than segregate, encrypt, and discard unnecessary communications like ThinThread did, Trailblazer "was about ingesting signals, identifying and sorting them, storing what was important, and then quickly retrieving data in response to queries." Eddington, *supra* note 45 (quoting MICHAEL V. HAYDEN, PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERROR 20 (2017)). This kind of data seizure and storage by the government violates the Fourth Amendment's right to be free from unreasonable search and seizure in the absence of a warrant and probable cause. U.S. CONST. amend. IV.

[48] Sinha, *supra* note 16, at 864.

[49] *Id.* at 888 ("[T]he NSA had 'intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress . . . .'") (quoting Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES (Apr. 15, 2009)), https://perma.cc/63UY-STSM. Sinha stated they used the term "NSA program" in their article to refer to what was publicly known as the "Terrorist Surveillance Program" and, internally at the NSA, as "Operation Stellar Wind." *Id.* at 876 n.79.

[50] Katherine Wong, *The NSA Terrorist Surveillance Program*, 43 HARV. J. ON LEGIS. 517, 519 (2006).

[51] *See* Letter from Attorney Gen. Alberto R. Gonzales to Senators Patrick Leahy and Arlen Specter (Jan. 17, 2007), https://perma.cc/V8G4-69M6; *NSA Timeline 1791-2015*, *supra* note 41; T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM*, VERGE (July 17, 2013, 1:36 PM), https://perma.cc/357Q-YX47; Sam Biddle, *The NSA Worked to "Track Down" Bitcoin Users, Snowden Documents Reveal*, INTERCEPT (Mar. 20, 2018, 11:22 AM), https://perma.cc/7K5Z-YPW5; *Newly Disclosed N.S.A. Files Detail Partnerships with AT&T and Verizon*, N.Y. TIMES (Aug. 15, 2015), https://perma.cc/ZES4-XB6P.

2007,[52] which decimated protections for U.S. persons by allowing warrantless surveillance of communications, so long as the communication was "directed at" someone overseas.[53]

A year later, Congress passed the FISA Amendments Act of 2008.[54] Constitutional rights advocates like the ACLU warned that these amendments continued to facilitate data-collection abuses against Americans.[55] The amendments broadened presidential powers by allowing mass spying of communications without requiring that targets had connections to terrorist activities or organizations;[56] restricted judicial oversight by allowing programs denied by FISC to continue;[57] and provided "retroactive immunity to the telecommunications companies for their role in the president's domestic spying program."[58] This immediately worried groups of lawyers, journalists, and human rights organizations like the ACLU and Amnesty International, which were concerned their communications with persons overseas would be intercepted. These groups claimed they would need to take extra precautions to protect their overseas communications with those who would be considered suspect under these amendments and filed a lawsuit in federal court to enjoin enforcement of the amendments and hold them to be facially unconstitutional.[59] But rather than make a determination on the substance of the FISA amendments, the Supreme Court held that Amnesty International did not have a sufficient case in controversy for standing because its alleged harm was too speculative.[60] The dissent, however, considered the alleged "speculative" injuries to be injuries in fact.[61]

---

[52] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

[53] *See* Sottek & Kopfstein, *supra* note 51; *ACLU Analysis of the Protect America Act*, ACLU, https://perma.cc/N2AY-8QBZ (last visited Sept. 29, 2020).

[54] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

[55] *See Talking Points on the FISA Amendments Act of 2008*, ACLU, https://perma.cc/E4YF-3Z4E (last visited Sept. 29, 2020).

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] Clapper v. Amnesty Int'l, 568 U.S. 398, 406-07 (2013) ("Respondents also assert that they 'have ceased engaging' in certain telephone and e-mail conversations. According to respondents, the threat of surveillance will compel them to travel abroad in order to have in-person conversations. In addition, respondents declare that they have undertaken 'costly and burdensome measures' to protect the confidentiality of sensitive communications.") (citations omitted).

[60] *Id.* at 402 ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").

[61] *Id.* at 422, 431, 441 (Breyer, J., dissenting).

B. The Wave of Backlash Comes Crashing Down

While much of the USA PATRIOT Act has received heavy criticism,[62] section 215—pertaining to the acquisition of business records—has been particularly controversial.[63] The constitutional right to privacy, specifically under the Fourth Amendment, considers whether an individual has a reasonable expectation to privacy; the reasonableness decreases as the individual moves farther away from the home.[64] The third-party doctrine—the principle that there is no reasonable expectation to privacy when one voluntarily provides information to a third party—bolsters the argument that seizing third-party documents does not violate any individual's right to privacy.[65] Supreme Court jurisprudence on the legality of bulk data collection, while considerate of the role technology plays in privacy, "does not provide a clear legal standard for when the Fourth Amendment applies to data shared with a third party . . . ."[66]

The combination of a sprawling data landscape, with underdeveloped legislative protection and minimal judicial oversight,[67] has allowed for the NSA's "dragnet surveillance of the domestic communications" that have *connections* to overseas terrorist activity.[68] A New York Times article from 2005 brought attention to the Terrorist Surveillance Program's "captur[ing] what are purely domestic communications in some cases, despite a requirement . . . that one end of the intercepted conversations take place on foreign soil . . . ."[69] In 2013, Edward Snowden

---

[62] *See, e.g.*, Lind, *supra* note 22; *Surveillance Under the USA/Patriot Act*, *supra* note 23. *See generally* Pike, *supra* note 24.

[63] *See e.g.*, Lind, *supra* note 22.

[64] Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1926-27 (2017).

[65] *Id.* at 1928-29.

[66] Sharon Bradford Franklin, Carpenter *and the End of Bulk Surveillance of Americans*, LAWFARE (July 25, 2018, 11:36 AM), https://perma.cc/QRS9-7BHR. *See also* Carpenter v. United States, 138 S. Ct. 2206, 2220-21 (2018) (holding a warrant is required when police seek cell phone tower data in connection with alleged criminal activity from a third-party); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that installing a GPS device in the defendant's car without a warrant constituted an unlawful search under the Fourth Amendment).

[67] *See* BRENNAN CTR. FOR JUSTICE, U.S. SURVEILLANCE: UNCHECKED AND UNSUPERVISED (2013), https://perma.cc/L7U7-EW6C.

[68] *NSA Spying*, ELEC. FRONTIER FOUND., https://perma.cc/7YGM-YH6Q (last visited Nov. 8, 2020).

[69] James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES (Dec. 21, 2005), https://perma.cc/7HE6-BGT9.

leaked[70] a court order directed at Verizon that exposed how extensive the NSA's surveillance program was.[71] PRISM was exposed as being an NSA and FBI tool used to grab data directly from private online service providers, like "Microsoft, Google, Apple, Yahoo, and others."[72]

Under the FISA Amendments Act, provisions like section 702[73] enabled backdoor programs like PRISM to exist for the purpose of collecting e-mails, phone data, and other telecommunications for foreign intelligence.[74] Acting under section 215 of the USA PATRIOT Act, the NSA "collected the telephone records from millions of Verizon customers," according to one of the revelations from the Snowden leaks.[75] The Privacy and Civil Liberties Oversight Board, an independent government agency, was enacted to analyze the executive branch's anti-terrorism decisions and ensure the consideration of individual liberties in those decisions.[76] In a 2014 review, the Board found the telephone surveillance programs provided no direct contribution "to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."[77]

In 2015, responding to the backlash, Congress passed—and President Obama signed—the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act

---

[70] While the Snowden leaks were not the first to expose the government's domestic spying, his revelations were the culmination of outdated privacy laws combined with the increased technological capabilities of government spying. *See* John Cassidy, *Snowden's Legacy: A Public Debate About Online Privacy*, NEW YORKER (Aug. 20, 2013), https://perma.cc/53J2-BAE6.

[71] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://perma.cc/G6DC-4RCR (describing an order from the NSA requiring Verizon to provide the agency with information on all telephone calls in Verizon's systems on an "ongoing, daily basis.").

[72] Sottek & Kopfstein, *supra* note 51.

[73] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436.

[74] *See Decoding 702: What Is Section 702?*, ELEC. FRONTIER FOUND., https://perma.cc/9KHX-DKLV (last visited Sept. 19, 2020); *see also 'Incidental,' Not Accidental, Collection*, ELEC. FRONTIER FOUND., https://perma.cc/PY9G-ZBVH (last visited Dec. 14, 2020).

[75] Greenwald, *supra* note 71; *see also* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2012 THROUGH 2014 (2016), https://perma.cc/39BW-8BQ6; Paul Szoldra, *This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, BUS. INSIDER (Sept. 16, 2016, 8:00 AM), https://perma.cc/HGP4-XRAX.

[76] *History and Mission*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., https://perma.cc/6CNU-NWBV (last visited Dec. 29, 2020).

[77] DAVID MEDINE ET AL., PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 11 (2014), https://perma.cc/S4ET-TLGF.

("USA FREEDOM Act" or "Freedom Act").[78] After some of the USA PATRIOT Act's more controversial provisions (e.g., section 215) had sunsetted, the Freedom Act brought them back with narrower requirements for the NSA to follow.[79] For instance, under the Freedom Act, the government must obtain permission from FISC before requesting communications records; additionally, the government cannot engage in bulk data grabs and is instead limited to specific search requests.[80] The Freedom Act also reined in the National Security Letters provision, essentially giving it the same restrictions that section 215 received.[81] In practice, though, these restrictions did not significantly affect the government's abilities to request bulk metadata.[82] And under the Freedom Act, these provisions were set to expire in December 2019; however, they have been reauthorized as recently as March 2020.[83] In fact, the latest decision to allow these provisions to stay intact came during the beginning of the COVID-19 lockdowns in the United States, on March 16, 2020.[84]

II. NATIONAL SECURITY AND PUBLIC HEALTH SURVEILLANCE DURING COVID-19

The United States got its first confirmed case of the novel coronavirus on January 21, 2020.[85] On February 26, the Centers for Disease Control and Prevention (CDC) identified the first U.S. case of COVID-19 where the patient had neither traveled to an outbreak area nor had a history of contact with an infected person.[86] While west coast states (e.g., Washington, California) were the first to attract national attention, it quickly

---

[78] USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

[79] Lind, *supra* note 22.

[80] *Id.* ("The USA Freedom Act would force the government to ask the Foreign Intelligence Surveillance Court for approval before being able to access phone records, and would only give it access for specific searches—not just passive bulk collection of everyone's data.").

[81] *Id.* ("[T]he government couldn't use the letters to get data they were banned from getting through the courts.")

[82] *See* Sharon Bradford Franklin, *Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records*, JUST SECURITY (Mar. 28, 2019), https://perma.cc/4V8B-W3RN ("But even with the [telecommunications providers rather than the government] holding the data and conducting the queries, the replacement [call detail records] program still permits the government to collect vast amounts of data . . . .").

[83] *See* Franklin, *supra* note 82; India McKinney, *House Lawmakers Extend Section 215 into Next Year Even Though They Had Years to Stop Illegal Overcollection of Americans' Sensitive Data*, ELEC. FRONTIER FOUND. (Nov. 19, 2019), https://perma.cc/6JH3-32LR; Margaret Taylor, *What Happened to FISA Reform?*, LAWFARE (Mar. 17, 2020, 3:06 PM), https://perma.cc/5VQ4-5CRR.

[84] Taylor, *supra* note 83.

[85] Erin Schumaker, *Timeline: How Coronavirus Got Started*, ABC NEWS (Sept. 22, 2020, 11:55 AM), https://perma.cc/QTM7-RXFE.

[86] *Id.*

shifted to New York, the epicenter of the U.S. outbreak.[87] This attention-shifting moved to the southern and midwestern United States as different states enacted varying levels of re-openings.[88] Former President Donald Trump declared a national emergency on March 13, 2020.[89] Not long after, the federal government sought broader powers during this state of emergency. For instance, only eight days after then-President Trump's emergency declaration, the Department of Justice requested the ability to "detain people indefinitely without trial during emergencies."[90]

A. Background on the Data Changes Since 9/11

Before delving into COVID-19 data surveillance, it is important to establish the data scene that currently exists, as compared to what existed post-9/11. The kind of technology that existed immediately following 9/11 was generally limited.[91] The percentage of U.S. adults who own cell phones has jumped from 62% in 2002 to 96% in 2019.[92] Smartphones, which actively and passively connect to the internet, have vastly increased the volume of data—specifically location data—on individual users.[93]

Legislation for electronic communications has existed since the 1980s but does not meet the needs of our present data-scape. Section 2703(d) of the Stored Communications Act, a law governing the voluntary and compelled disclosure of electronic communications held by third-party service providers, requires only that non-content information be "relevant and material to an ongoing criminal investigation"—a lower standard than a warrant requires—to compel production.[94] Jurisprudence has been underdeveloped as well. It was not until 2018, in *Carpenter v.*

---

[87] *Id.*

[88] *See* Lauren Aratani, *South and West Drive Record-Breaking Surge in Coronavirus Cases Across US*, GUARDIAN (July 11, 2020, 2:08 PM), https://perma.cc/6BAA-S53M; *see also* Reed Abelson, et al., *The Midwest Sees a Spike as Covid-19 Cases Decline Elsewhere*, N.Y. TIMES (Sept. 15, 2020), https://perma.cc/VE5K-26XY.

[89] *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak*, WHITE HOUSE (Mar. 13, 2020), https://perma.cc/D84N-7LTH.

[90] Betsy Woodruff Swan, *DOJ Seeks New Emergency Powers amid Coronavirus Pandemic*, POLITICO (Mar. 21, 2020, 1:01 PM), https://perma.cc/S6JQ-Q8SA.

[91] *See World Wide Web Timeline*, PEW RES. CTR. (Mar. 11, 2014), https://perma.cc/5N5R-JBU6.

[92] *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://perma.cc/AAB2-DMYY.

[93] *See* Stuart A. Thompson & Charlie Warzel, *Smartphones Are Spies. Here's Whom They Report to.*, N.Y. TIMES (Dec. 20, 2019), https://perma.cc/DT6H-TG7R.

[94] Sabrina McCubbin, *Summary: The Supreme Court Rules in* Carpenter v. United States, LAWFARE (June 22, 2018, 2:05 PM) (quoting 18 U.S.C. § 2703(d) (2018)), https://perma.cc/8QY9-H3B4.

United States, that the Supreme Court held a warrant was required to obtain aggregated cell-site location information (CSLI) from a third party during a criminal investigation.[95]

With shockingly little privacy precedent regarding aggregated cell phone location metadata combined with an unprecedented global health crisis, it is hard to predict the boundaries of future surveillance policy. Relaxed privacy standards that exist generally for third-party data collection compounded with a national crisis, where third-party data collection is necessary to stem the crisis, lead to the conclusion that those standards will only be further relaxed.[96]

Public health surveillance also uses big data, a practice that had been going on prior to the pandemic.[97] Among the goals of public health surveillance are "outbreak investigation, identifying newborns who need essential medical care, and research."[98] As heart disease and cancer started killing more people in the U.S. than infectious diseases, public health surveillance expanded beyond preventing infectious diseases and began identifying factors that cause chronic illnesses.[99] Public health surveillance now looks deeper into an individual's medical history to find genetic, behavioral, and environmental factors that could lead to chronic illness, rather than looking at surface symptoms connected to infectious diseases.[100] This bears likeness to the NSA's data collecting methodologies, as it also sweeps up large swathes of information.[101]

B. What Does Surveillance During the COVID-19 Pandemic Look Like?

Akin to how the NSA was central to anti-terrorism surveillance, the current pandemic requires the involvement of the U.S. Department of Health and Human Services (HHS) for data collection. The CDC, an agency within HHS, has stressed the importance of surveillance—coupled with shelter-in-place policies—to control and limit the spread of

---

[95] 138 S. Ct. 2206, 2210-11 (2018).

[96] *See* Joel, *supra* note 1; *see also* Swire, *supra* note 2.

[97] *Public Health Surveillance: Preparing for the Future*, CTRS. FOR DISEASE CONTROL & PREVENTION 7-11, 29-36 (2018), https://perma.cc/4B6Y-SZ8K.

[98] Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347, 351 (2007).

[99] *Id.* at 353-54 ("Today, surveillance programs exist for a variety of cancers, genetic conditions of newborns, and occupational diseases, as well as other health-related events like immunizations, injuries, and adverse drug reactions.").

[100] *Id.* at 354.

[101] *Id.* at 354-55 ("Case reporting is only one method of data collection. Other methods include population surveys, medical record reviews, and epidemiological and behavioral research studies aimed at determining the distribution, incidence, and causation of diseases across locations and populations, as well as the effects of prevention and treatment interventions.")

COVID-19.[102] History, too, holds examples of disease surveillance methods—albeit rudimentary ones—during pandemics. During the 1918 Spanish flu pandemic, white scarves tied on doors were used to identify which houses had people with infections;[103] and in 1854, John Snow's cholera map tracked the disease's progress, laying the groundwork for how we do the same today.[104] Though technology has changed, epidemiological surveillance (i.e., "the systematic collection, analysis, interpretation and timely dissemination of health data for the planning, implementation and evaluation of public health program[s]")[105] remains critically important to containing a disease.[106]

The post-9/11 era also utilized public health surveillance out of fear that a second wave of bioterrorist activity might occur.[107] Deaths resulting from anthrax mailed in letters[108]—as well as avian influenza[109] and the SARS epidemic[110] that soon followed—created anxiety that fueled the CDC's drafting of model legislation for mandatory disease reporting (e.g., the Model State Emergency Health Powers Act).[111] The CDC also proposed an increase in funding for federal bioterrorism grants to create surveillance programs.[112] Collection methods generally included case-reporting, population surveys, medical records reviews, and

---

[102] *See e.g.*, Press Release, Ctrs. for Disease Control & Prevention, CDC Launches New Weekly COVID-19 Surveillance Report (Apr. 3, 2020), https://perma.cc/8JL2-JW86.

[103] Julie Unruh, *Chicago Woman Shares Her Grandmother's Experience with the 1918 Spanish Flu*, WGNTV (Apr. 21, 2020, 10:35 PM), https://perma.cc/DJS5-GPJ5.

[104] Simon Rogers, *John Snow's Data Journalism: The Cholera Map that Changed the World*, GUARDIAN (Mar. 15, 2013, 5:30 AM), https://perma.cc/3J9H-DKE2.

[105] Steven B. Thacker et al., *A Method for Evaluating Systems of Epidemiological Surveillance*, 41 WORLD HEALTH STAT. Q. 11, 15 (1998), https://perma.cc/VDC3-MMTW.

[106] Mariner, *supra* note 98, at 361 ("Investigators needed to know within hours or days that highly contagious diseases . . . had been diagnosed in order to find the source of infection and investigate whether and where it might have spread. Only with quick access to such information could they protect others from imminent infection.").

[107] *Id.* at 356-57.

[108] *Timeline: How the Anthrax Terror Unfolded*, NPR (Feb. 15, 2011, 11:00 AM), https://perma.cc/9CDV-3FH6.

[109] Mariner, *supra* note 98, at 356.

[110] *Id.*

[111] Also known as MSEHPA, the draft legislation "increase[s] state powers to respond to bioterrorism or other outbreaks of disease that the [CDC] and others want the states to pass into law." *Model State Emergency Health Powers Act*, ACLU, https://perma.cc/F2QU-JG37 (last visited Nov. 7, 2020).

[112] Mariner, *supra* note 98, at 356-57.

epidemiological research.[113] While public health surveillance for purposes of national security is not a new concept, it will utilize the third-party, private internet industry in a unique way.[114]

Like the NSA did through its surveillance programs, the government is contracting with third-party software companies to do the tracing.[115] Contracting with private, third-party internet service providers allows for lower government regulation.[116] It also means the type of data being sought is considered "business records" (much like the post-9/11 surveillance era),[117] which provides greater ease of access to government officials.[118]

Before Google and Apple's contract to create contact tracing technology, Google's sister company, Verily, and its Project Baseline were touted by then-President Trump as a "front line player in the fight against a global pandemic."[119] The Baseline COVID-19 Program was developed "under the direction of the California Department of Public Health."[120] At the outset, users create a profile, take an online screener, and, if eligible, are directed to a testing site.[121] The Project Baseline website makes no mention of temporality when it discusses the storage of users' health data; but it acknowledges that a range of information provided by users (e.g., name, address, phone number, survey responses) may be disseminated to "third parties" (e.g., contractors, public health authorities, Google) and

---

[113] *Id.* at 354-55.

[114] *See generally* Brandom & Robertson, *supra* note 4 (discussing the creation of new technology for the purpose of aiding the government in collecting mass metadata and health data that is disseminated to individuals via their smartphones).

[115] *Id.*

[116] The General Data Protection Regulation (GDPR), a European data protection law, has shown how loose U.S. data protection law is regarding the private sector, as demonstrated by the U.S.'s struggles to comply with the E.U.'s higher standards for data protection. *See* Vincent Manancourt, *EU Court Ruling Strikes Hammer Blow to Transatlantic Data Flows*, POLITICO (July 16, 2020, 1:19 PM), https://perma.cc/ZKY3-CWLA. The U.S.'s laxer treatment of data protection has resulted in "European regulators . . . increasingly speaking out in favor of keeping data stored inside the bloc." Vincent Manancourt, *Demise of Privacy Shield May Be the End of U.S.-Europe Data Transfers*, POLITICO (Aug. 4, 2020, 11:34 PM), https://perma.cc/N25U-VE6D.

[117] Greenwald, *supra* note 71.

[118] *See* Lind, *supra* note 22 (discussing Section 215 of the USA PATRIOT Act, the "business records" provision).

[119] Douglas MacMillan et al., *Trump Announced Google Was Building a Virus Screening Tool. Then Someone Had to Build It*, WASH. POST (Mar. 16, 2020, 10:09 PM), https://perma.cc/E6RS-Y3W9. *See also Baseline COVID-19 Testing Program*, PROJECT BASELINE BY VERILY, https://perma.cc/2ERG-59HK (last visited Nov. 7, 2020).

[120] *What Is the Baseline COVID-19 Program?*, *COVID-19 FAQ*, PROJECT BASELINE BY VERILY, https://perma.cc/D9GS-63PR (last visited Nov. 7, 2020).

[121] *How Do I Get Tested?*, *COVID-19 FAQ*, PROJECT BASELINE BY VERILY, https://perma.cc/D9GS-63PR (last visited Nov. 7, 2020).

that Google's access to user data will be "limited to the purpose of providing [protective storage] services."[122] Soon after Verily launched, it had issues with reaching site capacity,[123] preventing users from scheduling testing appointments.[124] The survey Verily used also behaved unexpectedly after users responded to a question about whether they were experiencing symptoms and "caused confusion among people trying to use the site."[125] Furthermore, Verily required that its users create a Google profile before using its site, which added to the insecurity over privacy protections for user health data.[126] These issues, resulting from a website created in a rush to meet the promises made by former President Trump, made it "more clear than ever that the website Trump described is not what the American public will use to find coronavirus testing."[127]

Like the way the government compelled and contracted with private entities like Verizon and AT&T for surveillance under the USA PATRIOT Act,[128] the government is now contracting with software corporations, like Google, Apple, and Facebook.[129] Google and Apple made smartphone technology that relies on the voluntary input of a positive COVID-19 diagnosis.[130] The tech uses Bluetooth Low Energy (BLE)

---

[122] *Who Will My Data Be Shared With?*, *COVID-19 FAQ*, PROJECT BASELINE BY VERILY (last visited Nov. 7, 2020) https://perma.cc/D9GS-63PR.

[123] "In the context of networks, capacity is the complex measurement of the maximum amount of data that may be transferred between network locations over a link or network path." *Capacity*, TECHOPEDIA, https://perma.cc/8YL5-7XGB (last visited Aug. 30, 2020).

[124] Daisuke Wakabayashi & Natasha Singer, *Coronavirus Testing Website Goes Live and Quickly Hits Capacity*, N.Y. TIMES (Mar. 16, 2020), https://perma.cc/25XL-Z9PL.

[125] *Id.* (describing how users who responded "yes" to the question about experiencing symptoms found the site abruptly ended the survey, while those responding "no" were asked further questions about their "age, location and other factors").

[126] *Id.* ("Verily is rolling out its virus-screening tool at a moment when its parent company, Google, is facing intense scrutiny for it[s] push to acquire and analyze health data. A group of U.S. senators is looking into a deal that Google made with Ascension, the nation's second-largest hospital system, which gave the tech giant access to millions of medical records without patients' explicit knowledge or consent.") (first citing Ed Pilkington, *Warren and Group of Senators Demand Google Answer How It Will Use Medical Data*, GUARDIAN (Nov. 21, 2019, 10:39 AM), https://perma.cc/7WMU-DAH2; and then citing Natasha Singer & Daisuke Wakabayashi, *Google to Store and Analyze Millions of Health Records*, N.Y. TIMES (Nov. 11, 2019), https://perma.cc/A76M-F9VR).

[127] Adam Clark Estes, *The Google and Verily Coronavirus Websites Are Off to a Rocky Start*, VOX: RECODE (Mar. 23, 2020, 1:10 PM), https://www.vox.com/recode/2020/3/15/21180518/coronavirus-google-verily-website-testing-trump.

[128] Sottek & Kopfstein, *supra* note 51; Greenwald, *supra* note 71; Brendan Sasso, *Judge: Patriot Act Snooping Was Accepted by Phone Companies*, HILL (July 30, 2013, 2:29 PM), https://perma.cc/V2WC-7XKU.

[129] Brandom & Robertson, *supra* note 4.

[130] *See* Kari Paul, *Apple and Google Release Phone Technology to Notify Users of Coronavirus Exposure*, GUARDIAN (May 20, 2020, 6:51 PM), https://perma.cc/MQB8-6W6T ("'User adoption is key to success and we believe that these strong privacy protections are

transmissions to track user proximities without tracking their specific location in the way GPS data does.[131] In short, the technology:

> [P]ick[s] up the signals of nearby phones at 5-minute intervals and store[s] the connections between them in a database. If one person tests positive for the novel coronavirus, they could tell the app they've been infected, and it could notify other people whose phones passed within close range in the preceding days.[132]

The tech, released in May 2020, already has buy-in: "[Twenty-two] countries and several US states are already planning to build voluntary phone apps using their software."[133] Facebook has also rolled out an interactive COVID-19 map to show how many people have reported symptoms in one's county.[134] Facebook's data comes from a survey of over one million users that was conducted by Carnegie Mellon University researchers.[135]

Other countries have versions of these apps with varying pipelines to their respective governments. In China's fight against the disease's second wave, its government began tracking citizens by sorting their personal data "into color-coded categories . . . corresponding to their health . . . ."[136] In Singapore, the Trace Together app keeps a register of all individual users' contacts and informs any contact who has been in proximity of that user within two weeks if that user tests positive for COVID-19.[137] Israel is also directly tracking location data on citizens' cell phones.[138]

C. Emerging Criticisms

Ultimately, contact tracing may prove to be an untrustworthy form of metadata surveillance. The kind of BLE technology the apps use to

---

also the best way to encourage use of these apps,' [Apple and Google] said in a joint statement . . . .").

131 *See* Brandom & Robertson, *supra* note 4.

132 *Id.*

133 Paul, *supra* note 130.

134 *See* Aaron Holmes, *Facebook Just Released an Interactive COVID-19 Map that Shows How Many People Are Reporting Symptoms in Your Area*, BUS. INSIDER (Apr. 20, 2020, 10:06 AM), https://perma.cc/RL6W-7YEF.

135 *Id.*

136 *See* Ali Dukakis, *China Rolls Out Software Surveillance for the COVID-19 Pandemic, Alarming Human Rights Advocates*, ABC NEWS (Apr. 14, 2020, 6:30 AM), https://perma.cc/FV5W-QNMP.

137 Andrew Crocker et al., *The Challenge of Proximity Apps for COVID-19 Contact Tracing*, ELEC. FRONTIER FOUND. (Apr. 10, 2020), https://perma.cc/4QQZ-724L.

138 David M. Halbfinger et al., *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*, N.Y. TIMES (Mar. 18, 2020), https://perma.cc/JH3Q-GYLP.

conduct contact tracing has not proven reliable.[139] Nuances of contact will be lost—likely increasing false positives—because tracing proximity through Bluetooth does not consider factors like duration (i.e., how long people are in contact with one another) or spatial considerations besides distance (i.e., whether users are in different rooms but still close enough for their phones to register each other's location).[140] The apps also require voluntary compliance, which makes their potential for accuracy unreliable.[141]

Policies regulating health-data privacy also create issues of consent. HHS's first response to COVID-19 was to adjust its regulations under the Health Insurance Portability and Accountability Act (HIPAA) to accommodate surveillance programs.[142] The Clinton administration enacted HIPAA to regulate insurance coverage,[143] reduce healthcare fraud and abuse,[144] and mandate confidentiality for protected healthcare data,[145] among other things. Customarily, a patient's written authorization is required for Public Health Information (PHI) to be disclosed by a covered entity, except when disclosure is required in narrow circumstances.[146] Alex Azar, the former Secretary of HHS, relaxed certain privacy provisions under HIPAA.[147] For instance, patient consent is no longer required

---

[139] *See* Brandom & Robertson, s*upra* note 4.

[140] *Id.*

[141] "The first problem . . . is getting a meaningful number of people to install the app and make sure it's active as everyone makes their way through the world. Most countries have made app installation voluntary, and adoption has been low. In Singapore . . . adoption has been about 12 percent of the population. If the United States had similar adoption, you've now made your big contact-tracing bet on the likelihood that two people passing one another have both installed this app on your phone. The statistical likelihood of this is about 1.44 percent. (It could be higher in areas with greater population density or where the app was more widely installed.)." Casey Newton, *Why Bluetooth Apps Are Bad at Discovering New Cases of COVID-19*, VERGE (Apr. 10, 2020, 6:00 AM), https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health.

[142] *See* Heather F. Delgado et al., *Relaxing of HIPAA Laws During COVID-19 Pandemic*, NAT'L L. REV. (Mar. 18, 2020), https://perma.cc/LQH6-U9NG.

[143] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, §§ 102, 111, 110 Stat. 1936.

[144] *Id.* §§ 201-50.

[145] *Id.* § 264.

[146] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://perma.cc/MH7Y-7KAB (last updated July 26, 2013) ("A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.").

[147] Delgado et al., *supra* note 142 (explaining Secretary Azar's "limited waiver" of the HIPAA Privacy Rule).

in certain circumstances if the release of that information is *necessary*.[148] What is considered "necessary"—much like what was considered "significant" under the USA PATRIOT Act—can be subject to broad interpretation.[149]

Republican Senators Roger Wicker (MS), John Thune (SD), Deb Fischer (NE), Jerry Moran (KS), and Marsha Blackburn (TN), introduced the COVID-19 Consumer Data Protection Act (CCDPA) on May 7, 2020.[150] The bill's goal is to "regulate the data collected by coronavirus contact tracing apps,"[151] and it claims to give users agency over how their data will be collected and disseminated, like requesting the user's "affirmative express consent."[152] Other bill provisions would allow users to opt out of data collection, revoke their consent, and anonymize the data once the pandemic is over, along with other cybersecurity protection mandates.[153]

The bill, however, will likely be ineffective. For starters, the data anonymization provision covers only data that was collected for the purpose of coronavirus contact tracing and not other data swept up in the collection process.[154] The bill also bypasses other stronger privacy protections provided by the FCC and prevents states from enacting their own "stricter privacy protections in the absence of strong federal protections at the FTC."[155] Most egregiously, CCDPA does not provide a private right of action[156] for injured parties.[157]

---

[148] *Id.*

[149] *See* Sullivan, *supra* note 38.

[150] S. 3663, 116th Cong. (2020). *See also* Press Release, U.S. Senate Comm. on Commerce, Sci., & Transp., Committee Leaders Introduce Data Privacy Bill (May 7, 2020), https://perma.cc/TS3B-JJS6.

[151] Kim Lyons, *Senators' Plan for Reining in Contact Tracing Apps Doesn't Make a Lot of Sense*, VERGE (May 1, 2020, 2:08 PM), https://perma.cc/C2X8-VP9L.

[152] *See id.*; *see also* Press Release, U.S. Senate Comm. on Commerce, Sci., & Transp., *supra* note 150.

[153] Ashley Prickett Cuttino, *COVID-19 Consumer Data Protection Act Announced by Republican Senators*, NAT'L L. REV. (May 10, 2020), https://perma.cc/E3A9-JWAT.

[154] *See* Lyons, *supra* note 151.

[155] *Id. See also* Adam Schwartz, *Two Federal COVID-19 Privacy Bills: A Good Start and a Misstep*, ELEC. FRONTIER FOUND. (May 28, 2020), https://perma.cc/2ZKR-2VWY ("[The CCDPA] preempts state laws, has no private right of action, and exempts a broad set of surveillance by employers.").

[156] "Circumstances when a court will determine that a law that creates rights also allows private parties to bring a lawsuit, even though no such remedy is explicitly provided for in the law." *Definition*, *Private Right of Action*, QUIMBEE, https://perma.cc/2DHW-E7C4 (last visited Sept. 2, 2020).

[157] Schwartz, *supra* note 155.

Ten days after the CCDPA was introduced, Democratic Senators Richard Blumenthal (CT) and Mark Warner (VA), with Democratic Representatives Anna Eshoo (CA-18), Jan Schakowsky (IL-9), and Suzan DelBene (WA-1), introduced their own privacy bill, titled the Public Health Emergency Privacy Act (PHEPA).[158] PHEPA is considered more substantial regarding individual privacy protections than its Republican counterpart: "It requires opt-in consent and data minimization, and limits data disclosures to government. It has a strong private right of action and does not preempt state laws. And it bars denial of voting rights to people who decline to opt-in to tracking programs."[159] Even with these privacy protections championed by privacy experts, there are still weaknesses, including "broad exemptions for manual contact tracing, public health research, public health authorities, and entities regulated by [HIPAA]."[160] It also opens the door for potential discrimination—in areas like employment and education—should people decline to use tracking apps.[161]

Finally, a third bill, the Exposure Notification Privacy Act (ENPA), was introduced on June 1, 2020, by Senators Maria Cantwell (D-WA) and Bill Cassidy (R-LA).[162] This bill specifically targets data collected from "automated exposure notification service[s]," including contact tracing apps.[163] ENPA, like PHEPA, has a broad definition of the types of data it would protect,[164] but, like the CCPDA, it has a limited scope for a covered entity.[165] While narrowly confined to contact tracing apps, the scope of ENPA's application is not limited to the pandemic,[166] a positive sign when considering long-term privacy protections.

It is worth noting that not all the privacy legislation being passed during the pandemic is necessarily related to the pandemic. While the intent behind the above bills may seem to favor individual privacy rights,

---

158 S. 3749, 116th Cong. (2020); H.R. 6866, 116th Cong. (2020).

159 Schwartz, *supra* note 155.

160 *Id.*

161 *Id.*

162 S. 3861, 116th Cong. (2020).

163 *Id.* § 4(A).

164 Both PHEPA and ENPA protect data that is "linked or reasonably linkable to an individual," acquired through either "an[] individual or device," or "in connection with an automated exposure notification service," respectively. JONATHAN M. GAFFNEY, CONG. RESEARCH SERV., LSB10501, "TRACING PAPERS": A COMPARISON OF COVID-19 DATA PRIVACY BILLS 3 (2020), https://perma.cc/AU36-5KNU. Conversely, CCDPA protects only "precise geolocation data, proximity data, a persistent identifier, and personal health information." *Id.*

165 *Id.* at 2, 4. ("Under the CCDPA and ENPA, for example, a *covered entity* would include any entity or person engaged in a covered activity that is (1) subject to regulation by the Federal Trade Commission (FTC), (2) a common carrier as defined in the Communications Act of 1934, or (3) a nonprofit organization.").

166 *Id.* at 2 ("While the CCDPA and PHEPA apply specifically to the current COVID-19 pandemic, the ENPA is not limited to the current public health emergency.").

the Senate negated this gesture by attempting to renew the USA PATRIOT Act.[167] Soon after the renewal bill's announcement, then-Senate Majority Leader Mitch McConnell moved to amend the USA PATRIOT Act and allow the FBI to collect data on "Americans' web-browsing and search histories without a warrant."[168] While this amendment is not directly part of any COVID-19 public health surveillance programs, it clearly follows the post-9/11 pattern of taking advantage of a national crisis to strengthen the government's reach into the privacy sphere.

III: WHAT KINDS OF PROTECTIVE MEASURES WILL REDUCE THE POTENTIAL FOR PRIVACY VIOLATIONS?

The similarities between post-9/11 and COVID-19 surveillance were noticed almost immediately by the privacy community.[169] Once again, the government will use data collected from private, third-party corporations, and the laws governing individual users' privacy rights will not provide much protection. While these kinds of broad-sweeping, data-grabbing programs are a threat to any person, they disproportionately affect vulnerable communities in practice. Anti-Muslim ideology heavily influenced determinations of who became a target of NSA terrorist surveillance post-9/11.[170] And throughout the COVID-19 pandemic, Asian-American communities, specifically Chinese-American communities, have been subjected to varying acts of racism, including hate crimes.[171]

Racism in data surveillance is inevitable, as non-white communities maintain higher rates of infections and deaths from COVID-19.[172] Black Americans and other communities of color are already subject to much

---

[167] *See* Spencer Ackerman, *Mitch McConnell Moves to Expand Bill Barr's Surveillance Powers*, DAILY BEAST (May 13, 2020, 2:33 PM), https://perma.cc/8ULW-A3HP.

[168] Aaron Holmes, *Mitch McConnell Is Pushing the Senate to Pass a Measure that Would Let the FBI Collect Americans' Web-Browsing History Without a Warrant*, BUS. INSIDER (May 13, 2020, 4:09 PM), https://perma.cc/6JQS-CHXG; *see also* Ackerman, *supra* note 167 ("[The amendments] will expressly permit the FBI to warrantlessly collect records on Americans' web browsing and search histories.").

[169] *See, e.g.*, Joel, *supra* note 1; Swire, *supra* note 2.

[170] *See* Natasha Lennard, *The NSA's Racist Targeting of Individuals Is As Troubling as Indiscriminate Surveillance*, VICE (July 9, 2014, 2:40 PM), https://perma.cc/P2KN-XHD5.

[171] *See* Anna Purna Kambhampaty, *'I Will Not Stand Silent.' 10 Asian Americans Reflect on Racism During the Pandemic and the Need for Equality*, TIME (June 25, 2020, 6:32 AM), https://perma.cc/P9MJ-ERX2 ("Since mid-March, STOP AAPI HATE, an incident-reporting center founded by the Asian Pacific Policy and Planning Council, has received more than 1,800 reports of pandemic-fueled harassment or violence in 45 states and Washington, D.C.").

[172] *COVID-19 Cases, Hospitalizations, and Deaths, by Race/Ethnicity*, CTRS. FOR DISEASE CONTROL & PREVENTION (Nov. 30, 2020), https://perma.cc/8YX4-78XE.

higher rates of surveillance through local policing[173] and federal agencies like the FBI and NSA.[174] This kind of surveillance has gone hand-in-hand with justifying state-sanctioned violence and other aggressive control tactics against Black and Brown communities.[175] And it has already manifested during the COVID-19 pandemic: At the beginning of New York City's quarantine, there were disturbing differences in how the NYPD enforced social distancing on Black and Hispanic communities compared to white communities.[176]

Contact tracing policy must consider who will benefit from contact tracing and health data surveillance, given institutionalized medical racism and the general health disparities that racism creates for Black and Brown people overall.[177] Houseless people who cannot afford data plans, a severely at-risk population, will not have adequate access to contact tracing technology.[178] People in living conditions incompatible with digital contact tracing, like migrant workers sharing one mobile device or

---

[173] Chad Marlow & Gillian Ganesan, *Stop the Police Surveillance State Too*, ACLU (Aug. 19, 2020), https://perma.cc/3Y44-AX6Y ("Like policing itself, investigations into surveillance technology deployments have revealed, time and again, that they are overwhelmingly unleashed against communities of color.") (citations omitted).

[174] Following the Snowden leaks, the NSA disclosed they had spied on Dr. Martin Luther King, Jr. Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016, 5:55 AM), https://perma.cc/GA88-RV6Y ("A few months after the first Edward Snowden revelation, the [NSA] disclosed that it had *itself* wiretapped King in the late 1960s . . . . Across our history and to this day, people of color have been the disproportionate victims of unjust surveillance.").

[175] Dorothy Roberts & Jeffrey Vagle, Opinion, *Racial Surveillance Has a Long History*, HILL (Jan. 4, 2016, 5:11 PM), https://perma.cc/T44S-BQNS ("In the U.S., this system of structural surveillance emerges from a history of racism and white supremacy that links the use of deadly force by police against young black men and women to our systems of criminal justice, social programs and public health . . . . This complex system of overlapping surveillance regimes did not emerge overnight but through reactions to moments of crisis, eventually becoming permanent aspects of government and society over time.").

[176] *See e.g.*, Ashley Southall, *Scrutiny of Social-Distance Policing as 35 of 40 Arrested Are Black*, N.Y. TIMES (Nov. 30, 2020), https://perma.cc/BEB6-RSU2; Josiah Bates, *Police Data Reveals Stark Racial Discrepancies in Social Distancing Enforcement Across New York City*, TIME (May 8, 2020, 5:26 PM), https://perma.cc/P8KQ-MQB2 (stating 81% (304 of 347) of summonses "for violations of emergency procedures and acts liable to spread disease" were given to Black and Hispanic people).

[177] *See* Meghana Keshavan, *'The Direct Result of Racism': Covid-19 Lays Bare How Discrimination Drives Health Disparities Among Black People*, STAT (June 9, 2020), https://perma.cc/WQP4-JF64.

[178] Amos Toh & Deborah Brown, *How Digital Contact Tracing for COVID-19 Could Worsen Inequality*, JUST SECURITY (June 4, 2020), https://perma.cc/5XUM-93XH ("In the United States, many homeless adults who do have access to phones cannot afford data plans. Studies also show that they change cell phones and phone numbers frequently, complicating public-health interventions that require regular online contact.").

people in refugee camps experiencing unstable internet or internet blackouts, will not see the benefits of contact tracing technology.[179] If this technology is not able to assist people in high-risk communities, the dangers of broad surveillance do not justify the benefits.[180] It is vital to implement privacy protections to reduce the harm that, based on previous examples, will befall the most vulnerable.

Those who have made the comparison between 9/11 and COVID-19 have provided insight on applying the lessons we learned, post-9/11, to the current moment.[181] Key pieces of advice, gleaned from the literature then and now, include enforcing temporality (either in the surveillance laws or in the ways that data can be stored),[182] creating effective structures of oversight to enforce limitations on surveillance programs,[183] and providing full transparency to the individual whose data is being collected and disseminated so they know where that data is going and how it will be used.[184]

Congress has acted quickly to respond to COVID-19, as it did immediately after 9/11. As mentioned in Part II, CCDPA, PHEPA, and ENPA are three pieces of legislation, drafted shortly after the U.S. began its pandemic response, that address contact tracing privacy concerns.[185] Although PHEPA and ENPA contain promising aspects, rushed legislation made during a crisis requires "focused and balanced" updates as the crisis continues.[186] The USA PATRIOT Act had several provisions (e.g., Section 215) that sunsetted in May 2015.[187] Even though this section was essentially renewed via the Freedom Act with (allegedly) stricter limitations, the original provision was created with a sense of temporality.[188] Including provisions that sunset provides an avenue for more "thoughtful debate" afterwards[189] or even an end to the intrusive, once-needed data

---

[179] *Id.*

[180] *Id.* ("To increase public trust in contact-tracing apps, some governments have committed to digital contact tracing that protects the right to privacy. But this may not be enough to quell mounting concerns about their potential for surveillance, especially in countries where police and security forces operate with impunity.").

[181] *See, e.g.*, Joel, *supra* note 1; Swire, *supra* note 2; *see also* Nick Paton Walsh, *9/11 Saw Much of Our Privacy Swept Aside. Coronavirus Could End It Altogether*, CNN (May 16, 2020, 1:27 PM), https://perma.cc/5BXT-WWBU.

[182] *See* Joel, *supra* note 1; *see also* Lind, *supra* note 22.

[183] *See* Joel, *supra* note 1; Swire, *supra* note 2.

[184] *See* Joel, *supra* note 1; Swire, *supra* note 2.

[185] *See supra* pp. 52-54.

[186] *See* Joel, *supra* note 1.

[187] Lind, *supra* note 22.

[188] *Id.*

[189] *Id.*

policy altogether. The data are purportedly collected anonymously,[190] though truly anonymous data has little value,[191] especially when tracing the spread of disease through a population.[192] In fact, Android users are required to turn on their device location setting, enabling GPS, to use the contact tracing apps on their phone; this, perhaps obviously, causes trepidation in believing the software is "privacy preserving."[193] Even without GPS data, the aggregate of enough data points can identify a user, so the data should only be stored temporarily.[194]

There should be significant, external oversight—akin to the Privacy and Civil Liberties Oversight Board's oversight of the NSA—to ensure the collected data has been useful in preventing the spread of COVID-19. If the data has not proven useful, appropriate enforcement will be required to prevent the unnecessary collection of data. Contact tracing through BLE technology may also prove to be unreliable.[195] External bodies like the Department of Defense, Department of Justice, House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence, and FISC have the authority to investigate the NSA.[196] Protections under the Office for Human Research ensure that HHS complies with the law.[197] HHS can also be internally inspected by the Office of Inspector General.[198] These investigatory bodies should be regularly involved to make

---

[190] *See* Dylan Scott, *Contact Tracing, Explained*, VOX (May 4, 2020, 7:30 AM), https://www.vox.com/2020/5/4/21242825/coronavirus-covid-19-contact-tracing-jobs-apps.

[191] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010). ("Data can be either useful or perfectly anonymous but never both.").

[192] John Snow's cholera map was so successful, in part, because it visualized the geographic spread of disease. This example illustrates that geography and geo-data are inextricable from the tracing of a disease's movement. *See* Rogers, *supra* note 104.

[193] Natasha Singer, *Google Promises Privacy with Virus App but Can Still Collect Location Data*, N.Y. TIMES (July 20, 2020), https://perma.cc/RT3M-WVTH.

[194] *See* Jay Stanley, *How to Think About the Right to Privacy and Using Location Data to Fight COVID-19*, JUST SECURITY (Mar. 30, 2020), https://perma.cc/Z6HY-KETH ("Anonymization alone does not solve all privacy problems; such data can often be re-identified, for example, by tracing a person's movements to their home and workplace."); *see also* Carrie DeCell, *Can Governments Track the Pandemic and Still Protect Privacy?*, JUST SECURITY (Apr. 6, 2020), https://perma.cc/M2QN-5GNJ.

[195] *See* Newton, *supra* note 142.

[196] *See Oversight*, NAT'L SEC. AGENCY/CENT. SEC. SERV., https://perma.cc/XB7B-DUL6 (last visited Nov. 20, 2020).

[197] *See Compliance & Reporting*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://perma.cc/75TR-263F ("[The Office for Human Research Protections] has responsibility for oversight of compliance with the U.S. Department of Health and Human Services (HHS) regulations for the protection of human research subjects." (citing 45 C.F.R. pt. 46 (2018)).

[198] *See Office of Investigations*, OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., https://perma.cc/C4LM-BRJ6.

sure health data is being used correctly to prevent the spread of COVID-19 and not continuously collected when it serves no purpose. There could also be an investigatory commission (not like the Trump administration's coronavirus taskforce),[199] that retains regulatory authority to track and evaluate the government's response to COVID-19 as the pandemic continues in the future.[200]

When asking people to comply with contact tracing apps, it is imperative that there be full transparency as to where their information is going.[201] The revelations about the NSA's surveillance activities, like what Edward Snowden leaked or the decades of other surveillance projects,[202] have sowed Americans' distrust in state agencies.[203] The justification for keeping these programs secret, post-9/11, was to keep the intelligence out of enemy hands.[204] This justification, however, does not support government secrecy when invading individual privacy, as "[h]alf of Americans say they are not at all or not too confident that the federal government will keep their personal records safe from hackers or unauthorized users."[205] The Facebook surveys conducted by Carnegie Mellon researchers used for tracking are eerily reminiscent of the Cambridge Analytica surveys that manipulated users leading up to the 2016 presidential election and other elections globally.[206] These surveys could cause users to do a double-take, afraid that their responses will be sold by opportunistic third par-

---

[199] This taskforce was led by former Vice President Mike Pence, a partisan entity with almost no experience in public health. *See* Dan Diamond & Adam Cancryn, *How Mike Pence Slowed Down the Coronavirus Response*, POLITICO (Aug. 26, 2020, 4:35 AM), https://perma.cc/BK3W-TGJN.

[200] Oona Hathaway, *COVID-19 Shows How the U.S. Got National Security Wrong*, JUST SECURITY (Apr. 7, 2020), https://perma.cc/KA7X-98BW ("There should be a Commission styled on the 9/11 Commission to assess the failures of the U.S. government, both federal and local, to respond to the pandemic and to chart a better course forward.").

[201] Stanley, *supra* note 194 ("If the government obtains any data, it must be fully transparent about what data it is acquiring, and from where, and how it is using that data.").

[202] *NSA Timeline 1791-2015*, *supra* note 41.

[203] *See* A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RES. CTR. (June 4, 2018), https://perma.cc/VU3Q-6BST.

[204] *See* Joel, *supra* note 1. ("The enemy we are fighting today is not a terrorist organization or a hostile foreign government. Secrecy has no place in the war against that virus.").

[205] Colleen McClain & Lee Rainie, *The Challenges of Contact Tracing as U.S. Battles COVID-19*, PEW RES. CTR. (Oct. 30, 2020), https://perma.cc/EL3D-V7EK.

[206] See Matthew Rosenberg & Gabriel J.X. Dance, *'You Are The Product': Targeted by Cambridge Analytica on Facebook*, N.Y. TIMES (Apr. 8, 2018), https://perma.cc/Q9CT-49QK, for a general overview of the Cambridge Analytica scandal. *See also* Jina Moore, *Cambridge Analytica Had a Role in Kenya Election, Too*, N.Y. TIMES (Mar. 20, 2018), https://perma.cc/77M3-4FTS; Carole Cadwalladr, *Fresh Cambridge Analytica Leak 'Shows Global Manipulation Is Out of Control,'* GUARDIAN (Jan. 4, 2020, 11:55 AM), https://perma.cc/XFX4-W85K.

ties (e.g., Facebook) for their own financial gain. Full government transparency (especially when contracting with corporate third parties) will encourage user engagement and increase the potential for success. While HHS has relaxed HIPAA-related consent standards for covered entities when distributing PHI to Public Health Authorities (and in some instances to the media, family, and friends),[207] user-provided consent must be considered integral to the COVID-19 contact tracing apps.[208]

CONCLUSION

It is expected that an emergency situation will require a quick response, but sometimes that results in responses that are not appropriate for the emergency.[209] Surveillance will be an integral part of containing the coronavirus, but a common occurrence during national crises is for the executive branch to take advantage of the moment to create new and bold powers for the government, with little oversight.[210] This overstep was evident after 9/11, when the NSA intercepted communications and gathered metadata from millions of American consumers through third-party telephone and internet providers.[211] Many of those policies are still in place; and even though they were amended some,[212] there are still huge chasms for individual privacy rights to fall into.[213] Looking back at the policy decisions from the Bush administration—and the fallout from those decisions—will help create a safer legal space for the individual as the government attempts to create a safer physical space during the pandemic.

---

[207] Delgado et al., *supra* note 142.

[208] *See* Stanley, *supra* note 194 ("If location data is to be used, there must be strict policies ensuring that, whenever possible, the patient has consented to such uses . . . .").

[209] Swire, *supra* note 2. ("[Bruce] Schneier gets credit for coining the term 'security theater' in his 2003 book 'Beyond Fear.' The idea is that government agencies and others have an incentive to show they are 'doing something' to fight the crisis, even if a security measure doesn't actually improve security.").

[210] Elizabeth Goitein, *The Alarming Scope of the President's Emergency Powers*, ATLANTIC (Jan./Feb. 2019), https://perma.cc/G5V8-H5T4.

[211] *See* Greenwald, *supra* note 71; Sottek & Kopfstein, *supra* note 51.

[212] *See* Lackey & Pottinger, *supra* note 12; *see also Talking Points on the FISA Amendments Act of 2008*, *supra* note 55.

[213] *See* Schwartz, *supra* note 155.