STATEMENT OF

ELIZABETH GOITEIN
SENIOR DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY

HEARING ON

DIGITAL DRAGNETS: EXAMINING THE GOVERNMENT'S ACCESS TO YOUR PERSONAL DATA

JULY 19, 2022

Introduction

Chairman Nadler, Ranking Member Jordan, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice.

Technological advances have radically altered the balance of power between the government and the people when it comes to privacy rights.[1] To start with, Americans in the digital age generate far more recorded information than they ever did previously. Along with the explosive growth in the means of communication, almost every action we take—from making simple purchases at a grocery store to taking the bus to work—leaves a digital data trail. The government's technological ability to intercept that information, including through imperceptible means such as the use of Stingrays to simulate cell phone towers,[2] is also much greater than it has ever been. And sophisticated computer algorithms allow the government to tease highly sensitive information out of massive accumulations of seemingly innocuous data points in ways that would not have been possible just two decades ago.

But perhaps the most significant change wrought by technology is the degree to which our most personal information—or, at least, data that can be used to derive such information—is held by third parties. Cell phone companies, internet service providers, social media platforms, and app developers hold a treasure trove of information about each of us, some of which we are conveying without even knowing it. When accumulated and analyzed, this information can reveal the most intimate details of our lives: our associations, habits, and even beliefs.

This change has enabled the erosion of privacy rights once enshrined in the law. That's because the law—including the Fourth Amendment interpretations issued by the courts and the statutes passed by Congress—has entirely failed to keep up with technology when it comes to data held by third parties. Although the Supreme Court recently acknowledged that such information may qualify for protection under the Fourth Amendment, and although Congress acted decades ago to protect certain sensitive categories of third-party data, there are gaps and loopholes in these protections, and the government is exploiting them to collect Fourth Amendment-protected data without any legal process whatsoever.

Fortunately, there are steps Congress can take to close the legal loopholes enabling the government's use of third-party data to circumvent the Fourth Amendment. In my testimony today, I will elaborate on the legal shortfalls and discuss possible solutions.

I. The Law

Since 1967, the Fourth Amendment has been understood to apply whenever the government intrudes on a "reasonable expectation of privacy."[3] For decades, however, the protections that flowed from this analysis were artificially constrained by the "third-party doctrine." First

---

[1] *See generally* Orin S. Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment," *Harvard Law Review* 125 (2011): 476-543, https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol125_kerr.pdf.
[2] *See* "Cell-Site Simulators/IMSI Catchers," Electronic Frontier Foundation, accessed July 8, 2022, https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.
[3] *See* Katz v. United States, 389 U.S. 347 (1967).

articulated in *United States v. Miller* (1976)[4] and reiterated in *Smith v. Maryland* (1978),[5] the doctrine holds that a person loses any expectation of privacy in information that he or she voluntarily discloses to another—no matter how limited or necessary the disclosure.

Arguably, this doctrine never made much sense. Most of us do not understand "private" to mean "secret"; we don't assume that information is private only if we never share it with another living soul. Rather, we understand privacy to be about controlling when and with whom we share information. The fact that a person might choose to confide in a spouse, relative, or even a group of trusted friends does not mean that she wants or expects the information to be widely available to the public.

Nonetheless, whatever sense the third-party doctrine might have made in the 1970s when it was established, it is wholly untenable today. Documents once stored in a desk at home are now frequently backed up to the cloud, accessible to the cloud service provider. Letters once sealed against inspection by the U.S. Post Office have become texts or emails, sent and stored by the companies that provide those services. Searches through card catalogues in the local library have turned into internet searches, generating search and web browsing records stored by internet service providers. And while it was once possible to pay a private visit, our cell phones—and therefore, our cell phone service providers—know where we are at all times, whether we are visiting a public park, a therapist, or Alcoholics Anonymous. In short, it is virtually impossible to go 24 hours without disclosing highly sensitive information to the multitude of third parties that manage life in the digital world.

Often, we are disclosing information without realizing it. For instance, when we post photos, videos, or comments on social media platforms, we're aware that this content is visible to anyone to whom we have granted access. But we might not know that the act of posting this content generates "metadata"—basically, information about information—that may be collected and stored by the platform. For instance, the platform "knows" the IP address of the device we used to post the information and our location at the time of posting.[6] It is this information—the facts we don't even know we're disclosing—that frequently holds the most interest for government investigators.

The Supreme Court has begun the long process of bringing the Fourth Amendment in line with these new realities. In 2018, in *Carpenter v. United States*,[7] the Court held that police officers need a warrant to compel cell phone companies to turn over historical cell site information for a seven-day period. The Court concluded that individuals retain a reasonable expectation of privacy in that information despite "sharing" it with their cell phone companies. Its reasoning was essentially twofold. First, comprehensive geolocation information, unlike the items of information at issue in *Miller* (bank deposit slips) and *Smith* (phone numbers transmitted over a particular line), can reveal the most intimate details of a person's associations and activities—

[4] 425 U.S. 435 (1976).
[5] 442 U.S. 735 (1979).
[6] *See, e.g.*, "Information for Law Enforcement Authorities," Facebook, accessed July 8, 2022, https://www.facebook.com/safety/groups/law/guidelines (noting that law enforcement may obtain IP addresses with a § 2703(d) court order and location information with a warrant).
[7] 138 S. Ct. 2206 (2018).

what the Court referred to as "the privacies of life."[8] Second, disclosure of one's location though the use of a cell phone cannot fairly be described as "voluntary," given that the only alternative is to forego cell phone use and—along with it—participation in modern life.

Unfortunately, the holding in *Carpenter* is limited to the facts of that case. The Court expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party. There is no way to predict when cases involving other types of third-party collection might come before the Court. We might well have to wait many years to discover how the Court will apply the principles articulated in *Carpenter* to comprehensive communications metadata, internet search and web browsing histories, DNA analyses, and multiple other categories of highly sensitive data. The Court also refrained from opining on whether warrants would be required to obtain cell site location information in national security or foreign intelligence investigations. To the extent this data collection takes place under Executive Order 12333 (discussed below), courts might never have the opportunity to weigh in on this question.

To its credit, Congress was quicker than the Court to acknowledge the third-party data problem. In 1986, it passed the Electronic Communications Privacy Act (ECPA) to expand and update federal wiretapping laws to reflect new technologies and modes of communication. As part of ECPA, Congress enacted the Stored Communications Act (SCA), which addresses the privacy of communications-related information held by third parties.

The SCA's prohibitions and permissions apply to "electronic communications service" (ECS) providers and "remote computing service" (RCS) providers. The law prohibited such companies from voluntarily disclosing the contents of communications to anyone, with a handful of narrow exceptions.[9] But it also recognized the sensitivity of communications "metadata," decades before Edward Snowden's disclosures made the term a household word. The SCA barred ECS and RCS providers from voluntarily disclosing "record[s] or other information pertaining to a subscriber to or customer of such service" to "any governmental entity," again with a handful of exceptions.[10] For both content and metadata, the exceptions include disclosures to government entities pursuant to a warrant, court order, or subpoena, depending on the type of records sought.[11]

Notably, Congress chose to prohibit the disclosure of non-contents communications information to governmental entities only, while allowing disclosure to private persons or entities. Although there is little legislative history to explain this choice, it is evident that governmental access to private information raises unique concerns. The government—whether federal, state, or local—has a wide range of coercive powers over individuals. To list just a few: It can imprison them, deport them, levy civil fines on them, deny them public benefits, or deny them a license to

---

[8] *Carpenter*, 138 S. Ct. 2210 (quoting Riley v. California, 573 U.S. 373, 403 (2014) (internal quotation marks omitted)).

[9] 18 U.S.C. § 2702(a)(1) (2018). ECS providers are prohibited from disclosing the contents of communications only when held "in electronic storage," defined to include only those communications that have not been opened and are less than 180 days old. *Id.*, § 2703(a). The U.S. Court of Appeals for the Sixth Circuit, however, held that the government required a warrant to obtain the contents of emails more generally, and the executive branch has adhered to this ruling. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[10] 18 U.S.C. §§ 2702(a)(2)-(3).

[11] *Id.*, §§ 2702(b)(2), (c)(1).

practice their profession. Private entities lack this panoply of coercive powers. At an even more basic level, the government alone is subject to the Fourth Amendment.

This is not to say that there are no concerns with non-governmental parties' access to communications metadata or other personal information. To the contrary, such access represents a significant intrusion on Americans' privacy. And there are multiple purposes for which such access might be sought, including some that are far more troubling than just marketing consumer products to likely buyers. For instance, organizations supporting candidates for political office—or the candidates themselves—might use the data to target voters, potentially sending them disinformation or otherwise attempting to skew electoral outcomes.[12] Nonetheless, it is important to recognize that governmental access to Americans' personal information is different in kind from access by corporations, non-governmental organizations, or individuals.

Another law governing the acquisition of information held by third parties is the Foreign Intelligence Surveillance Act (FISA). Until 2020, FISA included an extremely broad provision known by the shorthand "Section 215," which allowed the government to obtain an order from the Foreign Intelligence Surveillance Court ("FISA Court") that would require third parties to turn over "any tangible thing" if the government could show relevance to an authorized foreign intelligence, counterintelligence, or international terrorism investigation.[13] Although the government has disclosed almost no information about how it has used the so-called "business records" provision, the term "any tangible thing" would certainly include records relating to communications, including geolocation information. In 2020, however, Section 215 expired after Congress could not muster enough votes to reauthorize it.[14]

The government can still obtain some categories of data held by third parties using other national security authorities,[15] including a set of provisions that allow the government to issue a type of subpoena called a national security letter (NSL). NSLs may be used to acquire certain communications-related, financial, and credit records.[16] The FBI has long argued that it should be allowed to obtain any and all electronic communications transaction records ("ECTR") using an NSL. The Department of Justice's Office of Legal Counsel, however, has opined that NSLs

---

[12] This is not a far-fetched hypothetical. In the 2020 presidential election, Cambridge Analytica, created when Steve Bannon approached wealthy conservative campaign donors to fund a political consulting firm, acquired personal data on 87 million Facebook users through a researcher at the University of Cambridge, in violation of Facebook's agreement with the researcher. The company contracted with the Trump campaign and used the data to create psychological profiles on potential voters so that the campaign could target political ads to them. *See* Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained With A Simple Diagram," *Vox*, May 2, 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram. Evidence has emerged that Cambridge Analytica, which worked for other political campaigns around the world, was involved in the dissemination of disinformation. *See* "'Cambridge Analytica Planted Fake News,'" British Broadcasting Corporation (BBC), March 20, 2018, https://www.bbc.com/news/av/world-43472347; Issie Lapowsky, "Cambridge Analytica Execs Caught Discussing Extortion and Fake News," *Wired*, March 19, 2018, https://www.wired.com/story/cambridge-analytica-execs-caught-discussing-extortion-and-fake-news/.

[13] USA PATRIOT Act, Pub. L. No. 107-56, § 215 (2001) (codified at 50 U.S.C. § 1861 (2018)), *allowed to sunset*, Pub. L. No. 116-69, § 1703(a) (2019).

[14] India McKinney and Andrew Crocker, "Yes, Section 215 Expired. Now What?" Electronic Frontier Foundation, April 16, 2020, https://www.eff.org/deeplinks/2020/04/yes-section-215-expired-now-what.

[15] FISA's pen-register/trap-and-trace provision, for instance, enables access to communications metadata. *See* 50 U.S.C. §§ 1841-46 (2018).

[16] *See* 18 U.S.C. § 2709 (2018); 12 U.S.C. § 3401 (2018); 15 U.S.C. § 1681u (2018).

may only be used to obtain a customer's name and address, length of service, and billing records—not, for instance, geolocation information collected and stored by cell phone companies.[17] The FBI has sought to convince Congress to expand the scope of NSLs, but Congress has declined to give the Department the authority to obtain this extremely sensitive information using just an administrative subpoena.

II. The Loopholes

The laws and holdings discussed above leave much of the third-party doctrine undisturbed. As noted, the Supreme Court's ruling in *Carpenter* extends only to geolocation information obtained in criminal cases. ECPA applies only to communications-related information held by ECS and RCS providers. Nonetheless, these rules would seem to afford protection against the government obtaining Americans' geolocation information without a warrant and other types of sensitive communications-related information without a court order or subpoena.

And yet, over the past two years, investigative journalists have revealed that federal agencies have quietly been paying data brokers to gain access to entire databases of personal information, including Americans' geolocation information, without any legal process whatsoever.[18] This phenomenon is not limited to one or two isolated incidents; the list of federal agencies that reportedly have bought access to Fourth Amendment-protected data includes the Federal Bureau of Investigation,[19] the Drug Enforcement Administration,[20] multiple components of the Department of Homeland Security[21] (including the Secret Service[22]), and the Department of Defense.[23] Even the Internal Revenue Service, according to the Wall Street Journal, "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."[24]

---

[17] *See* Daniel L. Koffsky, *Requests for Information Under the Electronic Communications Privacy Act (November 5, 2008)*, in Opinions of the Office of Legal Counsel 32 (2008): 145-158, https://www.emptywheel.net/wp-content/uploads/2015/12/081105-FBI-ECPA-opinion.pdf.

[18] For a thorough examination of this practice, along with its legal and policy implications, *see* Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Center for Democracy & Technology, December 9, 2021, https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[19] *See* Sara Morrison, "A surprising number of government agencies buy cellphone data records. Lawmakers want to know why," *Vox*, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.

[20] *See id*.

[21] *See* Paul Blest, "ICE Is Using Location Data From Games and Apps to Track and Arrest Immigrants, Report Says," *Vice*, February 7, 2020, https://www.vice.com/en/article/v7479m/ice-is-using-location-data-from-games-and-apps-to-track-and-arrest-immigrants-report-says.

[22] *See* Joseph Cox, "Secret Service Bought Phone Location Data from Apps, Contract Confirms," *Motherboard* (*Vice*), August 17, 2020, https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.

[23] *See* Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Data Without Warrants, Memo Says," *New York Times*, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

[24] Byron Tau, "IRS Used Cellphone Location Data to Try to Find Suspects," *Wall Street Journal*, June 19, 2020, *https*://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.

Nor are these small-ticket purchases. Over three years, DHS's Customs and Border Protection (CBP) reportedly spent $1 million to obtain location information from the data broker Venntel.[25] The amount of information CBP has obtained as a result of this arrangement is massive. According to documents recently obtained by the ACLU in response to a Freedom of Information Act request, CBP obtained 113,654 location points over a three-day period in 2018 for just one area in the Southwestern United States.[26] Although more is known about the practice at the federal level, state and local law enforcement also have been caught buying information about social media users from data vendors.[27]

In using data brokers to obtain Americans' private information, government agencies have taken advantage of a vast and shadowy industry that has grown exponentially in recent years. The data market, valued at $200 billion per year,[28] is diffuse, with well-known brokers—like the credit-reporting bureaus Experian, Equifax, and TransUnion—operating alongside firms with varying specialties that function with minimal publicity or transparency.[29] The brokers' clients are equally diverse, encompassing marketing firms, hedge funds, insurance companies, and other data brokers.[30] The information often is sold from company to company, so that the entity that originally generates the information (for instance, a particular app developer) is unaware of the identity of the end user (for instance, a particular government agency), and vice versa.

Data brokers obtain information from a wide variety of sources. In some cases, brokers pay app developers to install code that collects raw geolocation data and transmits it to the brokers.[31] Other methods include purchasing data from app developers or a broad range of other companies (e.g., financial institutions and retailers) that collect and maintain customer information; using cookies to track online activity; or scraping information from public-facing sites—often in violation of the host's terms of service.[32] Through such means, companies can assemble "thousands of attributes each for billions of people"—information that can be used to determine "if you've just gone through a break-up, if you're pregnant or trying to lose weight, whether you're an extrovert, what medicine you take, where you've been, and even how you swipe and tap on your smartphone."[33]

---

[25] *See* Blest, "ICE Is Using Location Data."
[26] *See* Shreeya Tewari and Fiyako Walter-Johnson, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data," ACLU, July 18, 2022, https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data.
[27] *See* Kristina Cooke, "U.S. Police Used Facebook, Twitter Data to Track Protestors: ACLU," Reuters, October 11, 2016, https://www.reuters.com/article/us-social-media-data-idUSKCN12B2L7.
[28] David Lazarus, "Shadowy Data Brokers Make the Most of Their Invisibility Cloak," *Los Angeles Times*, November 5, 2019, https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[29] *See id.*
[30] *See* Jenny Ross, "Privacy Update: How the Federal Government Buys Our Cell Phone Location Data," *Decentralize Today*, July 11, 2022, https://dt.gl/how-the-federal-government-buys-our-cell-phone-location-data/.
[31] *See* Bennett Cyphers, "App Stores Have Kicked Out Some Location Data Brokers. Good, Now Kick Them All Out," Electronic Frontier Foundation, March 10, 2021, https://www.eff.org/deeplinks/2021/03/apple-and-google-kicked-two-location-data-brokers-out-their-app-stores-good-now#:~:text=Data%20brokers%20entice%20app%20developers,governments%20all%20around%20the%20world.
[32] *See* Steven Melendez and Alex Pasternack, "Here Are the Data Brokers Quietly Buying and Selling Your Personal Information," *Fast Company*, March 2, 2019, "https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information; Franklin, Nojeim, and Thakur, *Legal Loopholes and Data for Dollars*, at 10-12.
[33] Melendez and Pasternack, "Here Are the Data Brokers Quietly Buying and Selling Your Personal Information."

In their marketing materials, data brokers boast about the dizzying number of people whose information they collect and sell, and how revealing that information is. The firm Near has described itself as "The World's Largest Dataset of People's Behavior in the Real-World," with location data representing "1.6B people across 44 countries."[34] The website for broker X-Mode (now renamed Outlogic) claimed that its data covered "25%+ of the Adult U.S. population monthly."[35] Venntel marketed its services to DHS by claiming that it collects 15 billion location points from over 250 million cell phones and other mobile devices every day,[36] noting that this information can be used to "identify repeat visitors, frequented locations, pinpoint known associates, and discover pattern [sic] of life."[37]

It is no surprise that data brokers are marketing their products to government agencies. The question is: Given the Supreme Court's holding in *Carpenter*, how is it lawful for the government to obtain Americans' cell phone location information—sometimes in massive quantities—without any legal process, let alone a warrant? The apparent answer, at least in part, is that agency lawyers have interpreted *Carpenter* to apply only when the government *compels* companies to disclose location information.[38] When the government merely *incentivizes* such disclosure—by writing a big check—the warrant requirement simply disappears. At that point, the government may obtain this Fourth Amendment-protected information in unlimited quantities without any individualized suspicion of wrongdoing, let alone probable cause and a warrant.

This tendentious interpretation has set off a slew of investigations, both by agencies' Inspectors General and by Congress.[39] However, those investigations could take time, and on their own they are unlikely to result in any change in the government's practices. Inspectors General can recommend changes but cannot enforce their recommendations, while Congress presumably would need to follow its investigation with legislative action. Furthermore, challenging this interpretation in court will be difficult. Americans are not notified when their personal information is purchased by government agencies, and so any given plaintiff would likely have trouble establishing standing to sue. All in all, it appears that the government's legal sophistry has effectively sidelined the Fourth Amendment for the time being.

---

[34] Jon Keegan and Alfred Ng, "There's a Multibillion-Dollar Market for Your Phone's Location Data," *Markup*, September 30, 2021, https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

[35] *Id*.

[36] *See* Tewari and Walter-Johnson, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data."

[37] Venntel, "Mobile. Location. Intelligence." Accessed July 17, 2022, 1, https://www.aclu.org/sites/default/files/field_document/production_3_reprocessed_jan._22.pdf#page=25 (document obtained by the ACLU through the Freedom of Information Act (FOIA), included on pages 25-26 or CBP-2020-033428-0000260 and -0000261 of the compiled production document).

[38] *See* Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants"; Hamed Aleaziz and Caroline Haskins, "DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People," BuzzFeed News, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[39] *See* Byron Tau, "Homeland Security Watchdog to Probe Department's Use of Phone Location Data," *Wall Street Journal*, December 2, 2020, https://www.wsj.com/articles/homeland-security-watchdog-to-probe-departments-use-of-phone-location-data-11606910402.

That leaves us with the protections Congress has provided. Cell phone location information held by cell phone service providers clearly falls within the term "record or other information pertaining to a subscriber to or customer of such service," as stated in ECPA. Cell phone companies are thus prohibited from disclosing such information to the government without a court order or subpoena.

ECPA, however, is woefully outdated. The law applies only to providers of electronic communications and remote computing services, and those terms are defined to encompass the third parties that were in the business of storing Americans' communications-related information when the law was passed in 1986. Applied today, the terms cover phone companies, internet service providers, providers of email and text messaging services, and social media platforms (although ECPA explicitly excludes messages that are "readily accessible to the general public"[40]). However, they do not reach a wide range of app developers, nor do they extend to digital data brokers. That definitional shortfall was not a conscious choice by Congress; rather, the entities in question simply didn't exist when Congress wrote the law.

This gap creates an easy end-run around the law's protections. Companies that are prohibited from selling their data to the government can simply sell it to a data broker—a disturbingly common practice[41]—and the data broker can resell the same information to the government, at a handsome profit. The information is effectively laundered through a middleman. Alternatively, app developers that are not covered by ECPA may sell data directly to the government, although in practice, they are more likely to operate through data brokers as well.

There is an even wider gap in FISA. As noted above, Section 215, which gave the government broad authority to obtain records from third parties with an order from the FISA Court, expired in 2020. Unlike ECPA, however, that authority was not paired with a prohibition against companies disclosing the records *without* a FISA Court Order. FISA states that its provisions provide the "exclusive means" for conducting "electronic surveillance."[42] But "electronic surveillance" is defined to include only the capture of communications content; it does not include many types of records containing communications metadata and other sensitive non-contents information, such as geolocation data.[43]

It is thus likely that the government is continuing to obtain Americans' geolocation information in foreign intelligence investigations without any statutory authority whatsoever. When the government collects foreign intelligence information outside of FISA or other statutes, it is be limited only by Executive Order (EO) 12333 and implementing policies.[44] EO 12333 contains far weaker constraints than FISA, and surveillance under the order is not subject to any judicial

[40] 18 U.S.C. § 2511(2)(g)(i) (2018).
[41] In 2020, for example, Federal Communications Commission Chairman Ajit Pai proposed fines totaling $208 million after major mobile phone carriers like T-Mobile, Verizon, and Sprint were caught selling their consumers' real-time location data to data brokers without their knowledge or consent. *See* Jon Brodkin, "Senate Bill Would Ban Data Brokers from Selling Location and Health Data," *Ars Technica*, June 15, 2022, https://arstechnica.com/tech-policy/2022/06/senate-bill-would-ban-data-brokers-from-selling-location-and-health-data/.
[42] 50 U.S.C. § 1812 (2018).
[43] *Id.,* § 1801(f) (2018).
[44] United States Intelligence Activities, Exec. Order No. 12333, 3 C.F.R. 200 (1981).

oversight.[45] In 2020, when Congress was debating the reauthorization of Section 215, Senator Richard Burr—who then chaired the Senate Select Committee on Intelligence—warned that if Section 215 expired, "the president under 12333 authority can do all of this without Congress's permission, with no guardrails."[46]

EO 12333 would not prevent the National Security Agency, the Central Intelligence Agency, or the FBI from buying access to databases that include Americans' most personal information. Indeed, it is quite possible this is already happening. In 2021, through the efforts of Senators Ron Wyden and Martin Heinrich, the public learned that the CIA was engaged in bulk collection of an unspecified type of data, and that the agency was searching through this data for Americans' information.[47] The CIA has refused to provide any public information about this practice beyond acknowledging its existence and issuing broad statements about its general authorities. It is thus impossible to know whether this "bulk collection" occurred through the purchase of commercially available data. However, it is a reasonable guess, given the ready availability of such data compared with other potential methods of obtaining it.[48]

The data broker pipeline also serves as a workaround for the limitations on the authority conferred by NSLs. As noted above, Congress has declined to provide the FBI with the authority to obtain geolocation information and other sensitive types of communications data using NSLs, which require no judicial review. Using data brokers, however, the FBI can obtain geolocation information without meeting even the low substantive and procedural bars required to issue an NSL.

When agencies obtain data from brokers, it generally comes in anonymized or aggregate form. Yet the removal of identifying information from the data offers little protection for individuals' privacy. Studies have shown that it is surprisingly easy to de-anonymize the data provided by brokers, with university researchers routinely able to re-identify upwards of 90% of the information.[49] For sophisticated actors like the Defense Intelligence Agency (one of the known consumers of geolocation data[50]), de-anonymization is child's play.

This testimony has focused largely on geolocation and communications-related information, given its sensitivity and the intense governmental interest in obtaining it. But there are various laws limiting third parties' disclosure of other types of data—for instance, the Health Insurance Portability and Accountability Act and the Financial Modernization Act. These laws, too, have

---

[45] *See generally* Faiza Patel and Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, Brennan Center for Justice, March 16, 2016, https://www.brennancenter.org/our-work/research-reports/overseas-surveillance-interconnected-world.

[46] "Sen. Burr claims EO 12333 permits mass surveillance 'without Congress's permission,'" C-SPAN video, 00:18, March 12, 2020, https://www.c-span.org/video/?c4860932/user-clip-sen-burr-claims-eo-12333-permits-mass-surveillance-without-congresss-permission.

[47] *See* Charlie Savage, "C.I.A. Is Collecting in Bulk Certain Data Affecting Americans, Senators Warn," *New York Times*, February 10, 2022, https://www.nytimes.com/2022/02/10/us/politics/cia-data-privacy.html.

[48] For an incisive analysis of what the CIA's bulk collection program is likely to entail, see Julian Sanchez, "CIA's Bulk Collection of American Records," CATO Institute, February 18, 2022, https://www.cato.org/blog/cias-bulk-collection-american-records.

[49] *See* Natasha Lomas, "Researchers spotlight the lie of 'anonymous' data," *TechCrunch*, July 24, 2019, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.

[50] *See* Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants."

gaps that would give the government easy access to personal information through data brokers. For one thing, they apply to health plans or health care providers[51] and financial institutions[52]—not necessarily to apps that may collect similar information about your health or finances. In addition, these laws protect only personally identifiable information;[53] they place few restrictions on the disclosure of anonymized or aggregate data, which, as noted, can easily be de-anonymized. Health care institutions[54] and banks[55] alike have taken advantage and begun selling their customers' information to data brokers.

The government's ability to evade privacy protections for geolocation information and other categories of highly sensitive data raises enormous concerns. The Fourth Amendment is not only a safeguard for civil liberties, but equally—and essentially—a safeguard for civil rights. Our government has a long history of using surveillance powers to target social justice movements, political opponents, and people of color.[56] However, when government officials must demonstrate individualized, fact-based suspicion of criminal activity in order to collect Americans' personal information, it is harder for them to fall back on conscious or subconscious prejudices—whether racial, ethnic, religious, or ideological. By contrast, when legal barriers to surveillance are missing or inadequate, we can expect to see a rise in the targeting of marginalized communities.

Data brokers offer a range of information that government agencies could use to target people based on factors like political affiliation or participation in racial justice movements. The data broker Oracle partners with a company called Affinity Answers to provide information on interest in political organizations (e.g., NAACP and Planned Parenthood), political media figures (e.g., Bill O'Reilly and Anderson Cooper), state-level political organizations, and politicians.[57] Another data broker, Geofeedia, used its access to social media platforms to track Black Lives Matter protesters and sold that information to police departments.[58] Fysical and SafeGraph, two

---

[51] 45 C.F.R. § 160.103 (2014).
[52] 15 U.S.C. § 6809(3) (2006).
[53] *See* 42 U.S.C. § 1320d-6 (2012); 15 U.S.C. § 6809(4) (2006).
[54] *See* Adam Tanner, "How Data Brokers Make Money Off Your Medical Records," *Scientific American*, February 1, 2016, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.
[55] *See* Associated Press, "Banks Profit From Selling Customers' Spending Data," *Courthouse News Service*, December 3, 2019, https://www.courthousenews.com/banks-profit-from-selling-your-spending-data/.
[56] *See generally* Elizabeth Goitein, Faiza Patel, and Frederick A.O. Schwarz, Jr., "Lessons From the History of National Security Surveillance," in *The Cambridge Handbook of Surveillance Law*, eds. David Gray and Stephen E. Henderson (Cambridge: Cambridge University Press, 2017), 553-76.
[57] *See* Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, Sanford School of Public Policy at Duke University, 2021, 7, https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.
[58] *See* Sam Levin, "ACLU Finds Social Media Sites Gave Data to Company Tracking Black Protesters," *Guardian*, October 11, 2016, https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter. In a promotional email, Geofeedia "invite[d] the Los Angeles District Attorney to learn how Baltimore used [Geofeedia's] software to monitor and 'stay one step ahead of the rioters' after the police killing of Freddie Gray." Nicole Ozer, "Police Use of Social Media Surveillance Software is Escalating, and Activists Are In the Digital Crosshairs," *ACLU of Northern CA* (blog), *Medium*, September 22, 2016, https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48#.fowkro6dy.

data brokers offering location data, mapped people attending the 2017 presidential inauguration.[59]

There is exceedingly little public information about what data the government is actually purchasing and how it is using that data. Federal agencies remain silent, even as the controversy intensifies. Nonetheless, there is already disturbing evidence that groups of people are being targeted based on constitutionally-protected characteristics. As noted, police departments have purchased data to assist in tracking racial justice protesters. In 2020, Vice News reported that the Department of Defense had purchased geolocation information generated by a popular Muslim prayer app used by more than 98 million Muslims around the world, including in the United States.[60] Many are also rightly concerned that state and local authorities, in states where abortion is now illegal, will use warrantlessly-acquired geolocation data—as well as information about women's reproductive health collected and sold by app developers—to identify women who seek abortions and health care providers who perform them.[61]

III. The Solutions

To safeguard the privacy of information held by third parties, Congress must act. A good starting point would be closing the loopholes in ECPA and FISA. Congress should pass legislation to ensure that the government cannot buy its way around the procedures those laws set forth for government acquisition of communications-related information, including geolocation information.

There is promising legislation pending in both chambers to accomplish this goal: the Fourth Amendment Is Not For Sale Act.[62] The bill is led in the Senate by Ron Wyden, and it has a long bipartisan list of cosponsors. In the House, it is led by the Chair of this Committee, Rep. Jerrold Nadler, along with Rep. Zoe Lofgren.

---

[59] *See* Jennifer Valentino-DeVries, et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[60] *See* Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[61] *See, e.g.,* Faiza Patel and Alia Shahzad, "With *Roe v. Wade* at Risk, Digital Surveillance Threatens Reproductive Freedom," *Just Security*, May 17, 2022, https://www.justsecurity.org/81547/with-roe-v-wade-at-risk-digital-surveillance-threatens-reproductive-freedom/. Illustrating the concern, one investigative news outlet paid data broker SafeGraph $160 for a week's worth of cellphone location information reflecting visits to clinics that offer abortions, including over 600 Planned Parenthood locations. *See* Joseph Cox, "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics," *Motherboard* (*Vice*), May 3, 2022, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood. Another company, Placer.ai, reportedly offered access to data caches and "heat maps" showing the approximate locations where people visiting Planned Parenthood clinics live. *See* Joseph Cox, "Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live," *Motherboard* (*Vice*), May 5, 2022, https://www.vice.com/en/article/g5qaq3/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placer-ai. Both companies pledged to stop these activities at the request of Senator Elizabeth Warren. *See* Office of Sen. Elizabeth Warren, "Warren Announces Two Key Data Brokers' Commitment to Permanently Stop Selling Location Data of People Seeking Abortion Services," July 7, 2022, https://www.warren.senate.gov/newsroom/press-releases/warren-announces-two-key-data-brokers-commitment-to-permanently-stop-selling-location-data-of-people-seeking-abortion-services. However, that is no guarantee that other companies are not engaging, or will not engage, in similar practices.

[62] H.R. 2738, 117th Cong. (2021); S. 1265, 117th Cong. (2021).

The bill would prohibit law enforcement or intelligence agencies from purchasing—or otherwise obtaining "in exchange for anything of value"—certain records obtained by third parties in certain ways. The covered records include the communications metadata described in ECPA, along with communications content and location information. Such records fall within the bill's prohibition as long as third parties have obtained them from ECS or RCS providers or intermediary service providers; from online accounts with ECS or RCS providers; from or about an electronic device; or in ways that result in unauthorized or deceitful access (e.g., in violation of terms of service).

With this legislation in place, law enforcement and intelligence agencies would be required to obtain court orders to access such information, using the same standards courts would apply when compelling disclosure from ECS or RCS providers. Other types of government agencies—such as public health or education departments—would still be able to purchase the data in question. However, the bill would prohibit them from sharing this information with law enforcement and intelligence agencies. Records obtained by law enforcement and intelligence agencies in violation of the law could not be introduced as evidence in any legal proceeding and would be subject to statutory minimization requirements.

The bill also attempts to close the gap in FISA coverage. It would amend FISA to state that its provisions are the exclusive means by which communications metadata may be obtained from an ECS or RCS provider for foreign intelligence purposes. In addition, the provisions of FISA that require the rough equivalent of a warrant—namely, a probable cause finding by the FISA Court that the subject of surveillance is a foreign power or agent of a foreign power—would become the exclusive means by which the government could obtain location information, web browsing history, internet search history, or any other records for which "compelled production . . . would require a warrant for law enforcement purposes."

The bill is not perfect. For one thing, it does not restrict disclosures by third parties that are not "in exchange for something of value." Data brokers are not good Samaritans, and they are in the business of making money. Nonetheless, one can imagine them occasionally sharing information with no charge because they believe it will serve their financial interests in the long run—by currying favor to avoid government regulation, for example, or by burnishing their public image through "pro bono" disclosures in high-profile investigations. Absent an expansive reading of "in exchange for something of value," such disclosures might well escape the bill's coverage. In addition, some of the bill's definitions, such as the definition of "online account," are still too tightly keyed to information that originates with ECS and RCS providers, leaving potential wiggle room for app developers. Similarly, the FISA "exclusive means" language applies to communications metadata only when acquired from an ECS or RCS provider. All of these flaws, however, can readily be fixed as the bill moves forward.

While the Fourth Amendment Is Not For Sale Act would make enormous strides toward filling the gaps in ECPA and FISA, it would not address similar gaps in the laws that protect other types of private data. Moreover, the privacy of Americans' data will continue to be at risk as long as companies are free to collect, maintain, and store troves of personal information—including information that is unnecessary for those companies to provide the services they market—and sell that information to data brokers and other non-governmental third parties. Ultimately, a

comprehensive solution will require data privacy legislation along the lines of the European Union's General Data Protection Regulation (GDPR).

Enacting such comprehensive legislation will be a heavy legislative lift. Congress should throw itself into that effort, but it will likely take time. It would be a mistake to postpone closing the gaps in ECPA and FISA until that process is concluded. As discussed above, there is some logic to ECPA's distinction between disclosures to the government and disclosures to non-governmental entities. The collection of sensitive data by law enforcement and intelligence agencies poses unique risks to our rights and liberties. Moreover, the type of information covered by the Fourth Amendment Is Not For Sale Act—especially geolocation information—is clearly of particular interest to the government. The problem tackled by this bill, in short, is an urgent one: unfettered and seemingly widespread governmental access to the most sensitive information we generate. Congress thus should move quickly to strengthen and advance the Fourth Amendment Is Not For Sale Act, even as it considers ways to address the myriad other threats to privacy that exist in the digital era.