VIRGINIA LAW REVIEW

VOLUME 110 OCTOBER 2024 NUMBER 6

ARTICLES

INDISCRIMINATE DATA SURVEILLANCE

Barry Friedman & Danielle Keats Citron***

Working hand-in-hand with the private sector, largely in a regulatory vacuum, policing agencies at the federal, state, and local levels are acquiring and using vast reservoirs of personal data. They are doing so indiscriminately, which is to say without any reason to suspect the individuals whose data they are collecting are acting unlawfully. And they are doing it in bulk. People are unlikely to want this personal information shared with anyone, let alone law enforcement. And yet today, private companies are helping law enforcement gather it by the terabyte. On all of us.

Our thesis is straightforward: the unregulated collection of this data must cease, at least until basic rule-of-law requisites are met. Any collection must be authorized by democratically accountable bodies. It

* Jacob D. Fuchsberg Professor of Law, New York University School of Law; Director, Policing Project, New York University School of Law. The authors are grateful for the feedback and input of many colleagues, including Emily Berman, Noah Chauvin, Jim Dempsey, Kristen Eichensehr, Andrew Ferguson, Max Isaacs, Jeff Jonas, Samuel Levine, Maria Ponomarenko, Daniel Solove, Vincent Southerland, Kathy Strandburg, Peter Swire, Matt Tokson, and Andrew Weissmann. And they would like to thank the many research assistants whose hard work contributed to this piece: Jack Bolen, Leila Chang, Eleanor Citron, Samuel Ellis, Megan Flynn, Maya Konstantino, YJ Lee, Madison Lahey, Nicole Mo, Chris Moore, Jeff Stautberg, and Yidi Wu. This work was produced with generous support from the Filomen D'Agostino and Max E. Greenberg Research Fund at New York University School of Law.

** Jefferson Scholars Foundation Schenck Distinguished Professor in Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow.

must be transparent. It must be based on clear proof of efficacy (that a legitimate purpose actually is being served). There must be protections that minimize or avoid harms to individuals and society. And, of course, there must be judicial review of whether indiscriminate bulk data collection is constitutional, either at all or with regard to specific programs.

The basis for this thesis is a first-of-its-kind review of instances, from the dawn of the Information Age, in which Congress acted on these very issues. Much of that history involves indiscriminate collection of data on Americans for reasons of national and domestic security, because national security represents the outer bounds of what law enforcement and intelligence agencies are permitted to do, and much of what is done in the name of national security is inappropriate for domestic policing. Yet, in incident after incident, Congress made clear that indiscriminate bulk collection of Americans' data is unacceptable, unlawful, and of dubious constitutionality. To the extent that such collection was permitted at all, Congress demanded the very requisites specified above. Today's indiscriminate bulk surveillance by federal, state, and local policing agencies violates virtually all of these congressionally established norms. It should cease, at least until the rule-of-law requisites are met.

INTRODUCTION

The Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, which allowed states to criminalize abortion and which generated huge controversy that ripples today, also directed attention to a seemingly incongruous matter: personal data.[1] To be specific, apps used to track menstrual cycles and other details of individuals' intimate lives.[2] The fear motivating the attention was that prosecutors would obtain the data in an attempt to prove that women had indeed aborted a fetus.[3]

This alarm was entirely justifiable—prosecutors already have sought private data for abortion prosecutions.[4] Still, there was something deeply naive about the sudden attention to law enforcement's collection of personal digital data.[5] For some time now, law enforcement has been gaining access to the most minute details of our personal lives: where we go and stay; with whom we text and chat; what we read and search; what

[1] 142 S. Ct. 2228, 2242–43 (2022); Philip Bump, The Patterns of Out-of-State Abortions, Wash. Post (Sept. 1, 2023, 4:48 PM), https://www.washingtonpost.com/politics/2023/09/01/patterns-out-of-state-abortions/ [https://perma.cc/F8ZP-36H2].

[2] Rina Torchinsky, How Period Tracking Apps and Data Privacy Fit into a Post-Roe v. Wade Climate, NPR (June 24, 2022, 3:06 PM), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps [https://perma.cc/4XCD-WTWQ]; Sara Morrison, Should I Delete My Period App? And Other Post-Roe Privacy Questions, Vox (July 6, 2022, 12:50 PM), https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion [https://perma.cc/3UCU-L2M8].

[3] Jay Edelson, Post-Dobbs, Your Private Data Will Be Used Against You, Bloomberg News (Sept. 22, 2022, 4:00 AM), https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you [https://perma.cc/E23W-DNMK]; see also Leah R. Fowler & Michael R. Ulrich, Femtechnodystopia, 75 Stan. L. Rev. 1233, 1237–38 (2023) (discussing how prosecutors and government officials could leverage consumer data to enforce abortion prohibitions or criminally prosecute users).

[4] Cat Zakrzewski, Pranshu Verma & Claire Parker, Texts, Web Searches About Abortion Have Been Used to Prosecute Women, Wash. Post (July 3, 2022, 9:20 AM), https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/ [https://perma.cc/UUB7-H9NS].

[5] Ryan Phillips, Infant Death Case Heading Back to Grand Jury, Starkville Daily News (May 9, 2019), https://www.starkvilledailynews.com/infant-death-case-heading-back-to-grand-jury/article_cf99bcb0-71cc-11e9-963a-eb5dc5052c92.html [https://perma.cc/D3Z9-39NR]; Grace Oldham & Dhruv Mehrotra, Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients, The Markup (June 15, 2022, 6:00 AM), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients [https://perma.cc/379S-92YA]. For Supreme Court cases expressing protection for intimate privacy, see Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (identifying a right to privacy for couples seeking to procure contraception); Stanley v. Georgia, 394 U.S. 557, 568 (1969) (holding that the First and Fourth Amendments protect the possession of "obscene material").

we say to digital assistants; what medical advice we seek; and which health providers we see.[6] At volume, all data becomes intimate data, and today, law enforcement is gathering it up by the terabyte.[7] On each and every one of us.

What the abortion decision did was bring the spotlight of public attention to what already is an extensive and deepening relationship between law enforcement and private actors, which has enabled indiscriminate data surveillance, in bulk. It's no secret that *private* actors collect vast amounts of data on each of us.[8] What is less widely known, but essential to understand, is the full extent to which that data can be, is, and will be shared with agents of the state. Some twenty years ago, Michael D. Birnhack and Niva Elkin-Koren called this "The Invisible Handshake."[9] Today, it is a full embrace.

This Article is about the acquisition by law enforcement of personal data *indiscriminately* and *in bulk*. "Indiscriminately" means it is acquired without the sort of lawful predicate—such as probable cause or reasonable suspicion—that typically limits when law enforcement may target individuals. "In bulk" captures how the technology and economics of the digital age enable policing agencies to gather this data on all of us, or any subset it chooses.[10] Today, policing agencies are acquiring access to the personal data of vast swaths of society, without regard to whether the targets of data acquisition are suspected of any unlawful conduct

[6] Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age 58–63 (2022); see infra Part I.

[7] Gabby Miller, Transcript: Senate Hearing on Protecting Americans' Privacy and the AI Accelerant, Tech Pol'y Press (July 12, 2024) (statement of Ryan Calo), https://www.techpolicy.press/transcript-senate-hearing-on-protecting-americans-privacy-and-the-ai-accelerant/ [https://perma.cc/Z87R-JXR5] ("AI is increasingly able to derive the intimate from the available."); Alicia Solow-Niederman, Information Privacy and the Inference Economy, 117 Nw. U. L. Rev. 357, 361 (2022) (exploring the implications of machine learning tools' ability to derive personal data from "aggregations of seemingly innocuous data"); see infra Part I.

[8] See, e.g., Carly Page, Hotel Giant Marriott Confirms Yet Another Data Breach, TechCrunch (July 6, 2022, 7:21 AM), https://techcrunch.com/2022/07/06/marriott-breach-again/ [https://perma.cc/Q2HF-8P5S]; Andrew Leahey, Equifax, Experian Must Pay More Than Pennies for Data Breaches, Bloomberg Tax (Feb. 21, 2023, 4:45 AM), https://news.bloombergtax.com/tax-insights-and-commentary/equifax-experian-must-pay-more-than-pennies-for-data-breaches [https://perma.cc/Q2HZ-HG5B].

[9] Michael D. Birnhack & Niva Elkin-Koren, The Invisible Handshake: The Reemergence of the State in the Digital Environment, Va. J.L. & Tech., Summer 2003, at 1.

[10] On the ability to collect data in bulk and the economics of storing it, see Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think 6–12 (2013).

whatsoever. And they are using artificial-intelligence-driven tools to develop vivid pictures of who we are, what we do, where we go, what we spend, with whom we communicate, and much, much more.[11] Make no mistake, the state has each of us under surveillance, and the extent and cohesiveness of that surveillance are growing by the day.

Although we know for certain this access to vast amounts of personal data is happening, far too few of the details are public because law enforcement and private parties are engaged in deliberate evasion to prevent our knowing. Through misleading procurement practices, memoranda of understanding ("MOU") mutually pledging nondisclosure, parallel construction (the act of hiding from courts how law enforcement gets its leads), and more, public-private partners effectively manage to assemble vast pools of data outside the public eye, thereby avoiding any oversight.[12]

What this Article demonstrates is that this sort of gathering of massive reservoirs of personal data about innocent people (to use a shorthand for those for whom there is no suspicion of wrongdoing) has been condemned by Congress and the broader society it represents time and again, and justifiably so. From the birth of the age of computerization, to the deeply problematic and nefarious conduct of government agents during COINTELPRO, to the secret collections of data by the National Security Agency as revealed by Edward Snowden, when Congress has been forced to act on this sort of indiscriminate data collection, it has ordered this practice to cease.[13] It is true, as we explain in Part III, that members of Congress, as well as state and local legislators, prefer to duck confrontations with law enforcement whenever they can—and they certainly do. But when compelled to act, Congress has made clear that the unregulated gathering of computerized dossiers endangers personal privacy and security, and risks unchecked government power. Such surveillance has chilled and destroyed constitutional rights exercised in the service of social change, has fallen particularly heavily on vulnerable and marginalized minorities, and has put way too much power in the hands of executive branch actors.[14]

Still, to be clear—and this is what makes the issue a difficult one—law enforcement access to digital reservoirs may serve important purposes.

[11] See infra Part I.
[12] Id.
[13] See infra Part II.
[14] Citron, supra note 6, at xvi.

Ever since the advent of the internet, crime has moved online. From those who steal our identities and empty our bank accounts, to those who threaten and stalk us, to those who would terrorize us or foment insurrection, crime is online and is itself driven by access to personal data.[15] Law enforcement needs to use digital tools of some sort to keep us safe from wrongdoing, and those may well require access to personal data—though even yet it remains open to question whether that should include the data of individuals suspected of nothing.

Society's goal should be a reasoned balance, but things now are seriously out of kilter. Working hand-in-hand with the private sector, policing agencies at the federal, state, and local levels are indiscriminately accessing vast reservoirs of personal data.[16] In the absence of regulation, this has made suspects of us all, and invited harms of the most grievous sort.[17]

Our thesis is straightforward: the current state of affairs must end. This is not necessarily to call for a ban on all indiscriminate bulk data-collection partnerships. As we've indicated, there are reasons some degree of collection might be advisable for safety's sake. Rather, what we do here is derive from congressional debates and critical legislative actions taken since the dawn of the Information Age a set of very basic rule-of-law requisites that must be met before indiscriminate data surveillance can continue. Collection must be democratically authorized, not left to policing agencies alone to decide. The fact of collection must be transparent, even if some particulars are not, for security reasons. There must be a clear showing that collection protects public safety. And there must be safeguards in place—among them antidiscrimination,

[15] See, e.g., Luke Barr, Americans Lost $10.3 Billion to Internet Scams in 2022, FBI Says, ABC News (Mar. 13, 2023, 4:27 PM), https://abcnews.go.com/Business/americans-lost-103-billion-internet-scams-2022-fbi/story?id=97832789 [https://perma.cc/7DQP-U9ZP]; Joshua Barlow, Naval Officer Charged with Harassment, Cyberstalking, Identity Theft Against Ex-Wife, WTOP News (Oct. 24, 2022, 4:59 AM), https://wtop.com/montgomery-county/2022/10/naval-officer-charged-with-harassment-cyberstalking-identity-theft-against-ex-wife/ [https://perma.cc/6SP2-MBGR]; Farah Pandith & Jacob Ware, Teen Terrorism Inspired by Social Media Is on the Rise. Here's What We Need to Do., NBC News (Mar. 22, 2021, 4:30 AM), https://www.nbcnews.com/think/opinion/teen-terrorism-inspired-social-media-rise-here-s-what-we-ncna1261307 [https://perma.cc/V62E-GVYS]; Rebecca Heilweil & Shirin Ghaffary, How Trump's Internet Built and Broadcast the Capitol Insurrection, Vox (Jan. 8, 2021, 5:00 PM), https://www.vox.com/recode/22221285/trump-online-capitol-riot-far-right-parler-twitter-facebook [https://perma.cc/52NQ-5YZX].

[16] See infra Part I.

[17] Id.

minimization, and retention limits—to mitigate or eliminate a number of obvious harms to privacy, personal security, equality, and overweening state power. And all of this must be open to constitutional scrutiny.[18] We are skeptical that much of today's indiscriminate bulk public-private surveillance will satisfy these tests. But our overarching point is that indiscriminate bulk collection of our data behind our backs must come to a halt, and if it occurs at all, it must proceed only by the terms set after open and transparent democratic debate. This is what congressional action, when it has occurred, teaches us.

As we write, it is an understatement to say these issues are at the forefront of national politics.[19] Congress is embroiled in debates over the limits on policing agencies purchasing personal data from data brokers.[20]

[18] The recent guidance to federal agencies by the Office of Management and Budget ("OMB") regarding the use of artificial intelligence is greatly consistent with much of what we argue for here. See Proposed Memorandum from Shalanda D. Young, Dir., Off. of Mgmt. & Budget, to the Heads of Exec. Dep'ts & Agencies, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence 10, 16, 18, 22 (2023) (requiring public input, transparency, a showing of efficacy, and detailed safeguards, with hopefully narrow exceptions for some law enforcement and national security activity); accord Joy Buolamwini & Barry Friedman, How the Federal Government Can Rein in A.I. in Law Enforcement, N.Y. Times (Jan. 2, 2024), https://www.nytimes.com/2024/01/02/opinion/ai-police-regulation.html [https://perma.cc/4U5V-UVSJ] (acknowledging OMB's requirements and urging closing of loopholes).

[19] Thanks to Noah Chauvin for enhancing our list of examples.

[20] In April of 2024, the House of Representatives passed the Fourth Amendment Is Not For Sale Act ("FAINFSA") by a vote of 219-199. See H.R. 4639—Fourth Amendment Is Not For Sale Act, Congress.gov, https://www.congress.gov/bill/118th-congress/house-bill/4639/all-actions [https://perma.cc/Z8XL-6JC7] (last visited Sept. 7, 2024). This bill would flatly prohibit some of the practices we describe. Joseph Cox, Bill That Would Stop the Government Buying Data Without a Warrant Passes Key Hurdle, Vice (July 19, 2023, 11:19 AM), https://www.vice.com/en/article/wxjgd4/fourth-amendment-is-not-for-sale-act-passes-committee [https://perma.cc/GVB6-6KK7]. The Protect Liberty and End Warrantless Surveillance Act, which incorporates FAINSFA in full, passed through the House Judiciary Committee by a vote of 35-2. H.R. 6570, 118th Cong. (2023); see also H.R. 6570—Protect Liberty and End Warrantless Surveillance Act of 2023, Congress.gov, https://www.congress.gov/bill/118th-congress/house-bill/6570/all-actions-without-amendments [https://perma.cc/3XJS-Y9XC] (last visited May 15, 2024). The bipartisan, bicameral Government Surveillance Reform Act exceeds even FAINFSA in the information it would protect. H.R. 6262, 118th Cong. (2023); S. 3234, 118th Cong. (2023). The House of Representatives, by voice vote, adopted the Davidson-Jacobs Amendment to the National Defense Authorization Act, which would have prohibited the Department of Defense from purchasing U.S. persons' protected information without a warrant. H.Amdt.256 to H.R. 2670, Congress.gov (July 14, 2023), https://www.congress.gov/amendment/118th-congress/house-amendment/256/text?s=3&r=5 [https://perma.cc/U8KM-X75W]. For an overview of the threat to privacy that data brokers present and an evaluation of certain legislative proposals, see Emile Ayoub & Elizabeth Goitein, Closing the

Section 702 of the Foreign Intelligence Surveillance Act recently was reauthorized, but only for two years rather than the typical five, and it encountered an especially rocky road in light of recent revelations of FBI overreach.[21] In the course of reauthorization, Section 702 proponents adopted some reforms and promised to systematically consider more.[22] The Office of the Director of National Intelligence ("ODNI") recently declassified a report on the Intelligence Community's use of commercially available information, the most salient part of which is a recognition that indiscriminate bulk collection of information involves highly personal information and that claiming its collection avoids constitutional or other concerns simply because it is "publicly" or "commercially" available is unpersuasive. ODNI called for top-to-bottom reconsideration of the issue.[23] The Federal Trade Commission brought an action in January of 2024 against data broker X-Mode Social for selling sensitive data obtained from phones without customer consent.[24] That

Data Broker Loophole, Brennan Ctr. for Just. (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole [https://perma.cc/S3H5-5T7U].

[21] See Biden Signs Reauthorization of Surveillance Program into Law Despite Privacy Concerns, NPR (Apr. 20, 2024, 9:54 PM), https://www.npr.org/2024/04/20/1246076114/senate-passes-reauthorization-surveillance-program-fisa [https://perma.cc/M5XF-LV5R] ("The reauthorization faced a long and bumpy road to final passage Friday after months of clashes between privacy advocates and national security hawks pushed consideration of the legislation to the brink of expiration."); see also Preston Marquis & Molly E. Reynolds, House Passes Section 702 Reauthorization, Lawfare (Apr. 16, 2024, 12:59 PM), https://www.lawfaremedia.org/article/house-passes-section-702-reauthorization [https://perma.cc/78RP-RGB8] (describing the two-year reauthorization as a "key concession" to ensure the bill's passage).

[22] On the nature of the reforms, see infra notes 252–56. A commission was established to "consider ongoing reforms." Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, § 18(c), 138 Stat. 885 (2024) (codified as amended at 50 U.S.C. § 1881a); see also David Aaron, Unpacking the FISA Section 702 Reauthorization Bill, Just Sec. (Apr. 18, 2024), https://www.justsecurity.org/94771/unpacking-the-fisa-section-702-reauthorization-bill/ [https://perma.cc/XE4T-MVM3]. The Chair of the Senate Intelligence Committee, Senator Mark Warner, acknowledged drafting problems with the reauthorization bill and promised to work towards improvements this summer. Noah Chauvin, Too Much Power for Spy Agencies, Brennan Ctr. for Just. (Apr. 23, 2024), https://www.brennancenter.org/our-work/analysis-opinion/too-much-power-spy-agencies [https://perma.cc/J438-M9P9]. One upshot of the fight was that the FISA reform bill will come to the House floor for passage by simple majority, rather than requiring a two-thirds vote as leadership originally had planned. See Marquis & Reynolds, supra note 21.

[23] Off. of the Dir. of Nat'l Intel., Senior Advisory Grp., Panel on Commercially Available Info., Report to the Director of National Intelligence 2 (Jan. 27, 2022) [hereinafter ODNI Report], https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [https://perma.cc/69EZ-2NK2].

[24] Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-

same month, Senator Ron Wyden forced the Intelligence Community to reveal it was buying Americans' location data by putting a hold on the nominee for Director of the National Security Agency until this information became public.[25]

Despite the apparent urgency of these issues, little (if any) progress is being made, in large part—we believe—because legislators are simply uncertain how to proceed. That is where we seek to intervene. Relying on past congressional actions, we provide a roadmap for Congress, as well as state and local legislative bodies, as to the minimum requirements that must be in place before indiscriminate bulk data collection can continue. (And even then, as we say, there must be judicial review.)

Although our aspiration here is to suggest a path toward sound regulation, we are quite certain that *absent* the very basic rule-of-law requisites identified repeatedly by Congress, courts should invalidate *all* such indiscriminate collection as unconstitutional. It is difficult to understand how a court could uphold such activity given that, for the most part, we don't even know what actually is happening. That is no doubt why courts, confronted with these issues, have tended to dispose of them on justiciability or other grounds rather than reaching the merits.[26] Still, it is unacceptable for courts simply to turn a blind eye to the degree of surveillance that is occurring. Our review of congressional debates, coupled with a constitutional argument one of us has advanced elsewhere,

events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data [https://perma.cc/2RNF-JBTP]. On May 1, 2024, the FTC released its final order against InMarket in which it prohibited the data aggregator from sharing or selling sensitive location data for advertising and marketing purposes. Press Release, Fed. Trade Comm'n, FTC Finalizes Order with InMarket Prohibiting It from Selling or Sharing Precise Location Data (May 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-inmarket-prohibiting-it-selling-or-sharing-precise-location-data [https://perma.cc/B6XR-578H].

[25] See Letter from Ron Wyden, U.S. Sen., to Avril Haines, Dir. of Nat'l Intel. (Jan. 25, 2024), https://www.wyden.senate.gov/imo/media/doc/signed_wyden_letter_to_dni_re_nsa_purchase_of_domestic_metadata_and_ftc_order_on_data_brokers_with_attachments.pdf [https://perma.cc/EHJ8-69ZH]; Charlie Savage, N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says, N.Y. Times (Jan. 25, 2024), https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html [https://perma.cc/5GVM-RXXR].

[26] See, e.g., ACLU v. Clapper, 785 F.3d 787, 823–24 (2d Cir. 2015) (declining to address whether the NSA's bulk data collection pursuant to Section 215 violated the Fourth Amendment); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402, 414, 418 (2013) (dismissing for want of Article III standing the claim that § 1881a of the Foreign Intelligence Surveillance Act of 1978 is unconstitutional); Schuchardt v. President of the United States, 802 F. App'x 69, 76–77 (3d Cir. 2020); Obama v. Klayman, 800 F.3d 559, 562 (D.C. Cir. 2015).

provides ample basis for striking down indiscriminate bulk data surveillance that is occurring in the absence of any regulation and without anything in the way of serious guardrails.[27]

On the other hand, the appropriate time to address the constitutionality of indiscriminate bulk data collection in the context of a specific legislative program is when the contours of that legislative program are known, including factors such as any evidence of the utility of the data collected, and the safeguards in place to protect individual interests.[28]

Part I of this Article sets the stage by explaining that indiscriminate bulk data collection by domestic policing agencies is rampant and expanding at warp speed due to deepening public-private data partnerships. Section II.A details the profound data grab that is occurring and explains how, with the assistance of private helpers, law enforcement is accomplishing what it likely could not on its own. Section II.B makes the case that what is occurring may be but the tip of the iceberg. Law enforcement and their private partners are engaging in evasive (and dubiously constitutional) tactics to keep secret the fact that any of this is happening, making it impossible to know the true extent of the indiscriminate data surveillance.

Part II is the heart of our argument. It documents that when Congress has been forced to confront indiscriminate bulk data collection about innocent individuals by intelligence and policing agencies, it has registered sharp disapproval; Congress typically has shut down the collection. To the extent that the legislature allowed any mass access to data, the data was safeguarded with protections that often were understood to be foundational and perhaps required by the Constitution. To be clear, Congress has not always acted in the face of complaints about mass collection of private data. Public choice theory confirms what our own eyes see—caught between claims of national security and law

[27] See Barry Friedman, Lawless Surveillance, 97 N.Y.U. L. Rev. 1143, 1204–14 (2022) (providing a constitutional argument of precisely this nature).

[28] In *Carpenter v. United States*, the Supreme Court barred warrantless collection of over six days of cell site location information, despite such collection ostensibly being permitted by the Stored Communications Act. 138 S. Ct. 2206, 2216–19 (2018). But the Court went no further. In that decision, the Chief Justice expressed the need to move cautiously, lest the Court "embarrass the future." Id. at 2220 (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)). Actual legislation will provide the Court with an opportunity to evaluate the specific protections it embodies, as well as government arguments about the utility of the data collected. See, e.g., Berger v. New York, 388 U.S. 41, 44 (1967) (evaluating constitutionality of wiretapping in context of New York's law); see infra notes 332–40 and accompanying text (discussing how decisions like *Berger* have led to further legislation).

enforcement imperatives (on the one hand), and popular unhappiness about private data collection (on the other), as well as its own keen awareness of the dangers, Congress often bends to pressure. But when Congress has been forced to act, indiscriminate bulk data collection about Americans suspected of nothing consistently has been deemed unlawful, of dubious constitutionality, and has been rejected. Congress has insisted instead on a set of quite obvious basic prerequisites, grounded in the rule of law. Part II traces this history up to the present day. Much of what we discuss in Part II concerns national security, which serves as a notable benchmark, because all concerned agreed that while certain surveillance activities may be permissible to protect national security, they are simply impermissible for domestic purposes.

Part III, relying on congressional insights of the past, turns to prescription for the present. Section III.A summarizes the rule-of-law requisites that surfaced repeatedly in congressional debates and actions, making abundantly clear that the ongoing domestic law enforcement data grab detailed in Part I violates these requisites. Indiscriminate data collection should not occur *at all* unless it is democratically authorized, transparent, based upon demonstrated efficacy, and bounded by essential safeguards to prevent things like discrimination, risks to personal security, and the accumulation of overweening governmental power. This goes for data collection conducted for the use of policing agencies at every level of government, federal, state, tribal, and local. Section III.B then tackles the hard question—which is how to make this happen in light of the game of hot potato that keeps both the judiciary and legislative bodies from doing their regulatory and adjudicative jobs. That Section identifies a set of mechanisms to address the problem. One is what historically has been a game of judicial / legislative give-and-take that allows each branch to push the other toward sensible resolutions. Another is a set of sunsets—coupled with disclosure requirements—to ensure periodic democratic review and reevaluation of data collection efforts to, among other things, weigh the efficacy and value of such collections against the intrusions they involve. The third is an intriguing, ongoing intercontinental game of chicken between the European Union and the United States that might accomplish the same, at least at the federal level.

Data, in our world, is a benefit and a curse. If we are not careful, the curse will trump the benefits in too many of our lives. Even if the threat is not immediately obvious, allowing government access to this much information about all of us is a prescription for tyranny. Eyes were opened

by the idea that government could not only criminalize our reproductive lives but pry into our virtual and physical bedrooms and bathrooms to discover any criminality. That particular fear is justified, but the threats extend far beyond it. It is essential that we do something, now, about policing and intelligence agency's massive indiscriminate collection of our personal data.

I. HOW LAW ENFORCEMENT—WITH HELP—IS COLLECTING EVERYONE'S PERSONAL INFORMATION

Policing agencies in the United States are collecting, accessing, analyzing, storing, and sharing literally billions of data points about large swaths of the population, if not everyone.[29] From what we know, the total surveillance of people's lives is underway.[30] Domestic policing agencies could not accomplish this alone—there is no way a single domestic agency could collect this volume of data from all over the country, and aggregate it, let alone develop the artificial intelligence tools that make analysis of the data possible. Fortunately for them, they do not have to. They have eager helpers.[31]

This Part details how domestic policing agencies are relying on public-private partnerships to collect data on every one of us and what we know about this practice, despite their tactics to avoid public scrutiny.

Start with the large data aggregators, such as RELX Group, Thomson Reuters, West, and Acxiom, which have dossiers on virtually everyone

[29] Hura Anwar, New Secret Tool Allows the Police to Trace Billions of Data Points from American User Devices, Digit. Info. World (Sept. 4, 2022, 12:01 AM), https://www.digitalinformationworld.com/2022/09/new-secret-tool-allows-police-to-trace.html [https://perma.cc/2XLB-GGVT].

[30] See infra Part II.

[31] License plate readers provide a sharp example. Vendors like Axon, Vigilant, and Flock collect license plate reads in many jurisdictions and combine them, making the data available to all agency users. Joseph Cox, Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras, Vice (Mar. 3, 2021, 10:31 AM), https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader [https://perma.cc/LCK2-K6UP]; Axon, Axon Partners with Flock Safety to Enhance Security for Cities and Neighborhoods, PR Newswire (Apr. 2, 2020, 7:30 AM), https://www.prnewswire.com/news-releases/axon-partners-with-flock-safety-to-enhance-security-for-cities-and-neighborhoods-301033947.html [https://perma.cc/PQ3X-EQ8K]. A company named Rekor is using machine learning tools to analyze billions of data points to alert law enforcement agencies to drivers whose habits suggest possible criminal activity. Thomas Brewster, This AI Watches Millions of Cars Daily and Tells Cops if You're Driving Like a Criminal, Forbes (Dec. 5, 2023, 2:03 PM), https://www.forbes.com/sites/thomasbrewster/2023/07/17/license-plate-reader-ai-criminal/?sh=1173d3e73ccc [https://perma.cc/9DA9-H6XF].

living in the United States.[32] Data brokers have more than *ten thousand* data points on any given person, including their addresses, life events (pregnancy, abortion, divorce), family members, friends, sexual orientation, gender identity, drug prescriptions, mental illnesses, chronic health conditions, medical procedures, online searches, browsing habits, purchases, political and religious affiliations, utility use, and biometric information.[33] Data brokers contract with federal, state, and local policing agencies to provide this information for sums that reach into the tens of millions of dollars.[34]

Then there are the specialized data brokers, who make available to law enforcement information about people's health, dating, biometrics, and other sensitive data.[35] Other companies sell policing agencies access to bulk internet metadata, which reveals Americans' browsing histories and "sensitive information such as what doctor a person sees, their religion or what dating sites they use."[36] Companies like Clearview AI sell access to bulk collections of people's faces—10 billion images scraped from the internet and made available to over 3,000 federal, state, and local

[32] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim & Dhanaraj Thakur, Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers 24–27 (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf [https://perma.cc/W76Z-T5DK]; Aaron Rieke, Harlan Yu, David Robinson & Joris von Hoboken, Open Soc'y Founds., Data Brokers in an Open Society 13–14 (Nov. 2016), https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf [https://perma.cc/5GKB-7BRT].

[33] Justin Sherman, Duke Univ. Sanford Cyber Pol'y Program, Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy 3 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/PHH7-WHSZ].

[34] Shenkman et al., supra note 32, at 7, 25 (describing the prevalence of such contracts and noting that the nature of the data purchased, its use, and potential privacy consequences are often obscured through the use of opaque or technical designations). For example, the Department of Homeland Security awarded a contract to Thomson Reuters in May 2021 with a potential value of $4.2 million. Id. at 25 n.16.

[35] Joanne Kim, Data Brokers and the Sale of Americans' Mental Health Data: The Exchange of Our Most Sensitive Data and What It Means for Personal Privacy 4–5 (Feb. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf [https://perma.cc/A6D4-PX9N].

[36] Joseph Cox, Here Is the FBI's Contract to Buy Mass Internet Data, Vice (Mar. 27, 2023, 9:00 AM), https://www.vice.com/en/article/dy3z9a/fbi-bought-netflow-data-team-cymru-contract [https://perma.cc/MQ75-VKV9].

government agencies.[37] The cars we drive have numerous computers, which report into manufacturers, and then brokers aggregate this information and make it available to police.[38]

One area in which law enforcement is a big customer is the aggregation and analysis of Americans' social media posts. Companies like Dataminr and Giant Oak analyze billions of user-generated posts on social networks.[39] The Secret Service purchased Babel Street's social network product, which monitors public posts on Facebook, Instagram, Snapchat, YouTube, and WhatsApp.[40] State police in Massachusetts and Michigan have contracts with ShadowDragon enabling access to streams of social media, dating sites, Amazon, and the dark web.[41]

[37] Will Knight, Clearview AI Has New Tools to Identify You in Photos, Wired (Oct. 4, 2021, 7:00 AM), https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/ [https://perma.cc/W5V4-6W6L].

[38] See generally Nicole Mo, Note, If Wheels Could Talk: Fourth Amendment Protections Against Police Access to Automobile Data, 98 N.Y.U. L. Rev. 2232 (2023) (explaining how law enforcement agencies obtain automobile data without a warrant). Data broker Otonomo sells real-time location data from tens of millions of cars around the world to any organization that makes an account on its platform. Id. at 2239 n.35, 2247 n.89. In 2020, the Department of Homeland Security renewed a contract with Berla, which sells tools that plug into cars and extract data directly, including phone and infotainment data like "[r]ecent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been." Id. at 2246.

[39] Sam Biddle, Elon Musk Fought Government Surveillance—While Profiting Off Government Surveillance, The Intercept (Mar. 25, 2024, 12:16 PM), https://theintercept.com/2024/03/25/elon-musk-x-dataminr-surveillance-privacy/ [https://perma.cc/2MUW-NE4D] (explaining that Dataminr's First Alert platform continuously monitors public activity on social media and other internet platforms for governmental customers including police departments and provides them with real-time alerts on desired topics); Sam Biddle, LexisNexis Is Selling Your Personal Data to ICE so It Can Try to Predict Crimes, The Intercept (June 20, 2023, 4:33 PM), https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates/ [https://perma.cc/MG9Y-7TP3]; Max Rivlin-Nadler, How ICE Uses Social Media to Surveil and Arrest Immigrants, The Intercept (Dec. 22, 2019, 8:00 AM), https://theintercept.com/2019/12/22/ice-social-media-surveillance/ [https://perma.cc/R347-AHX3].

[40] Joseph Cox, Secret Service Bought Phone Location Data from Apps, Contract Confirms, Vice (Aug. 17, 2020, 9:00 AM), https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street [https://perma.cc/8E92-EKRZ].

[41] Michael Kwet, ShadowDragon: Inside the Social Media Surveillance Software That Can Watch Your Every Move, The Intercept (Sept. 21, 2021, 5:03 PM), https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/ [https://perma.cc/LFU4-WJFZ]; see also Austin Williams, Report: Data Brokers Selling Personal Information to US Government, Private Entities, Foreign Governments, Fox 5 D.C. (June 15, 2023, 3:22 PM), https://www.fox5dc.com/news/report-data-brokers-selling-personal-information-to-us-government-private-entities-foreign-governments [https://perma.cc/F5BS-AEHZ]

And companies aggregate and sell our location data, the one type of data that the Supreme Court in *Carpenter v. United States* identified as especially revealing of intimate life.[42] What can be purchased today—five years later—is more revealing than the cell site location data at issue in *Carpenter*, because companies like Fog Data Science combine geolocation data with data from apps that reveal who we are via mobile device advertising identification numbers.[43] Location data brokers boast that their software lets purchasers see "how often people visit, how long they stay, where they came from, where else they go, and more."[44] Companies store years' worth of data on millions of Americans, which means that police partners can go back in time to trace a mobile device's whereabouts—the very sort of "retrospective" data *Carpenter* flagged as especially concerning.[45]

(reporting that U.S. policing and intelligence agencies are purchasing personal data that data brokers obtained from phones, web browsers, and cars).

[42] 138 S. Ct. 2206, 2217 (2018); see Matthew Tokson, Government Purchases of Private Data, 59 Wake Forest L. Rev. 269, 275 (2024) (arguing that many government purchases of private data violate the Fourth Amendment).

[43] The Location Data Market, Data Brokers, and Threats to Americans' Freedoms, Privacy, and Safety: Hearing on Pending Legislation Before the J. Comm. on Consumer Prot. & Pro. Licensure, 2023 Leg., 193d Sess. 7–8 (Mass. 2023) (written testimony of Justin Sherman, Senior Fellow and Research Lead, Duke Univ. Sanford Sch. of Pub. Pol'y). These are our device IDs or mobile advertising ID numbers (numbers assigned to mobile devices, which easily are traced to individuals given their predictable travels to home and work). Id. at 5. Fog Data Science has claimed that it has billions of data points about over 250 million devices. Bennett Cyphers, Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police, Elec. Frontier Found. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police [https://perma.cc/JV7K-LCTL].

[44] Patterns, SafeGraph Docs, https://web.archive.org/web/20220531230024/https://docs.safegraph.com/docs/monthly-patterns [https://perma.cc/UGE7-S3KR] (capture dated May 31, 2022). The quoted language was removed from the company's page sometime between August and October 2022—perhaps due to criticism of these practices—so the link provided uses the Wayback Machine to capture the page as of May 2022.

[45] See Joseph Cox, Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal, Vice (Aug. 25, 2020, 9:00 AM), https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs [https://perma.cc/CZ69-H5BZ] (noting that U.S. Customs and Border Protection paid nearly half a million dollars for a location database that allowed retroactive search by area or by device); Christopher Mims, Your Location Data Is Being Sold—Often Without Your Knowledge, Wall St. J. (Mar. 4, 2018), https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400 [https://perma.cc/EP8A-9SCX]; see also *Carpenter*, 138 S. Ct. at 2218 ("[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable."). The location data broker Outlogic, formerly X-Mode, contracted with the Internal Revenue Service and the Department of Homeland Security, among other federal

Although much of this data is purchased, policing agencies get access to the data in other, sometimes more troubling, ways. Companies like SpyCloud sell law enforcement reservoirs of personal data stolen by criminal hackers.[46] Some companies just hand over bulk data to law enforcement: no contracts necessary.[47] And sometimes, companies are compelled by law to collect the data and turn it over; an example is a Houston ordinance that requires bars, nightclubs, sexually oriented businesses, convenience stores, and game rooms to capture and retain video of the exterior of their premises, and turn it over to law enforcement when requested and without process.[48] Policing agencies lawfully obtain data from private entities for one use, then store it away for whatever future use they like.[49]

The immense scope of this all can be seen in the public-private "partnership" between the Drug Enforcement Agency ("DEA") and

agencies, and was recently blocked by the FTC from selling sensitive location data to private sector entities without express affirmative consent of consumers. Lee Fang, IRS, Department of Homeland Security Contracted Firm that Sells Location Data Harvested from Dating Apps, The Intercept (Feb. 18, 2022, 12:01 PM), https://theintercept.com/2022/02/18/location-data-tracking-irs-dhs-digital-envoy/ [https://perma.cc/NZ9J-DD9V]; Adam Schwartz, FTC Bars X-Mode from Selling Sensitive Location Data, Elec. Frontier Found. (Jan. 23, 2024), https://www.eff.org/deeplinks/2024/01/ftc-bars-x-mode-selling-sensitive-location-data [https://perma.cc/SQH9-VGKD].

[46] Joseph Cox, Police Are Buying Access to Hacked Website Data, Vice (July 8, 2020, 9:29 AM), https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud [https://perma.cc/H6K9-JJPQ].

[47] For example, money transfer companies including Western Union secretly and voluntarily provided the Department of Homeland Security with millions of records of Americans' money transfers from 2014 to 2019. Michelle Hackman & Dustin Volz, Secret Surveillance Program Collects Americans' Money-Transfer Data, Senator Says, Wall St. J. (Mar. 8, 2022, 2:04 PM), https://www.wsj.com/articles/secret-surveillance-program-collects-americans-money-transfer-data-senator-says-11646737201 [https://perma.cc/3VY2-MHPS]; see also Senator Calls for Probe of Mass Surveillance Tool Used by U.S. Law Enforcement, Reuters (Jan. 18, 2023, 5:15 PM), https://www.reuters.com/world/us/senator-calls-probe-mass-surveillance-tool-used-by-us-law-enforcement-2023-01-18/ [https://perma.cc/82AC-4L92] (discussing law enforcement access to a database of over 150 million money transfers, which was created as a part of a settlement between the Arizona Attorney General's Office and Western Union).

[48] Elizabeth Nolan Brown, Houston Says Businesses Must Install Surveillance Cameras and Cops Can View Footage Without a Warrant, Reason (Apr. 21, 2022, 9:30 AM), https://reason.com/2022/04/21/houston-says-businesses-must-install-surveillance-cameras-and-cops-can-view-footage-without-a-warrant/ [https://perma.cc/VCS8-PGXN].

[49] Sexual Assault Victim Says DNA from Her Rape Kit Used Against Her by Police: "I Want to See Justice," CBS News (Oct. 17, 2022, 11:15 AM), https://www.cbsnews.com/news/sexual-assault-victim-says-dna-from-her-rape-kit-used-against-her-by-police/ [https://perma.cc/797Z-87NB].

AT&T to conduct "Hemisphere," a program in which AT&T employees actually were located at law enforcement agencies in Los Angeles, Houston, and Atlanta to respond in real time to data requests.[50] Amid concern about AT&T gathering data on billions of calls and handing it over to the government, it seemed as though Hemisphere had been shut down. Yet, we now know that the program still exists, simply operating under a different name.[51] As described, the company "maintains and analyzes its own collection of bulk telephone metadata for billions of calls" so that in response to administrative subpoenas from the DEA (on which no judge signs off), it can quickly produce the requested information.[52] Pretty cozy indeed.[53]

Policing agencies purchasing or being given access to bulk personal data often argue that this poses no problem—constitutional, regulatory, or otherwise—for a variety of reasons. First, they say, the information is commercially available—any private entity or person could buy it, so why not the government? Second, they argue that people consent to turning over the data when they download and use apps and services. Third, they claim the data is anonymized and so no risk can be associated with it. Finally, they push to one side the Supreme Court's decision in *Carpenter*—one of the few judicial data points close to on point—claiming it was narrowly limited to cell site location information, thus inapplicable to anything else. And besides, *Carpenter* involved a subpoena and now they are just buying it (as though that somehow helps).[54] The arguments show a mission-driven blindness, if not willful

[50] Hemisphere: Law Enforcement's Secret Call Records Deal with AT&T, Elec. Frontier Found., https://www.eff.org/cases/hemisphere [https://perma.cc/38XL-U37Y] (last visited May 15, 2024).

[51] Letter from Ron Wyden, U.S. Sen., to Merrick B. Garland, Att'y Gen., U.S. Dep't of Just. (Nov. 20, 2023), https://www.wyden.senate.gov/imo/media/doc/wyden_hemisphere_surveillance_letter_112023.pdf [https://perma.cc/E224-QZC9] (confirming existence of the "Data Analytical Services" program); see also Off. of the Inspector Gen., Dep't of Just., A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data, at ii (2019) [hereinafter OIG Report], https://oig.justice.gov/reports/2019/o1901.pdf [https://perma.cc/AZK2-ZMUQ] (describing a DEA "Program C" that appeared to be Hemisphere).

[52] OIG Report, supra note 51, at ii.

[53] Id. at ii–iv; Zack Whittaker, DEA Says AT&T Still Provides Access to Billions of Phone Records, TechCrunch (Mar. 28, 2019, 12:08 PM), https://techcrunch.com/2019/03/28/hemisphere-phone-records/ [https://perma.cc/GL78-DU99].

[54] See ODNI Report, supra note 23, at 19–20; see also Bennett Cyphers, How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale, Elec. Frontier Found. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/how-law-enforcement-aroun

disregard, for why this sort of gold rush of data aggregation is problematic.

A recently declassified report from the Office of the Director of National Intelligence ("ODNI Report") regarding commercially available information ("CAI") casts doubt on the validity of these sorts of arguments, as well as the failure of federal intelligence agencies to comprehend the stakes.[55] The ODNI Report explains, "Today, in a way that far fewer Americans seem to understand, and even fewer of them can avoid, CAI includes information on nearly everyone that is of a type and level of sensitivity . . . that could be used to cause harm to an individual's reputation, emotional well-being, or physical safety."[56] The data can be deanonymized easily, and in fact would be of little value to many agencies were it not.[57] Yet, "[e]ven subject to appropriate controls, CAI can increase the power of the government's ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations."[58] For these reasons, the ODNI Report was unimpressed by the sorts of arguments outlined above.[59] The entire thrust of the report is that the Intelligence Community needs to reevaluate its entire approach to personal data being sold or given to government agencies.

ODNI could not be more correct about the harms of this widespread collection. They have been documented extensively, by us and by others, and so we merely note them here, with ample citations in the footnotes. Collection at this level threatens personal security and invades individual

d-country-buys-cell-phone-location-data-wholesale [https://perma.cc/V3LU-N647] ("The Fourth Amendment analysis shouldn't change depending on where the data comes from . . . ."); Bennett Cyphers & Aaron Mackey, Fog Data Science Puts Our Fourth Amendment Rights up for Sale, Elec. Frontier Found. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-data-science-puts-our-fourth-amendment-rights-sale [https://perma.cc/P9ZR-4QN4].

[55] ODNI Report, supra note 23, at 1–2.

[56] Id. at 2–3.

[57] Id. at 1 ("Although CAI may be 'anonymized,' it is often possible (using other CAI) to deanonymize and identify individuals, including U.S. persons."); see also Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701, 1703–04, 1731–32 (2010) ("Data can be either useful or perfectly anonymous but never both.").

[58] ODNI Report, supra note 23, at 11.

[59] ODNI declined to weigh in on the validity of the arguments, but it was hard to miss the undertone. See id. at 14 ("[Calling modern CAI] materially indistinguishable from traditional [publicly available information] 'is like saying a ride on horseback is materially indistinguishable from a flight to the moon.'" (quoting Riley v. California, 573 U.S. 373, 394 (2014))).

and group privacy.[60] It frequently leads to discriminatory outcomes because of biases of policing agencies that reach far back into history to the point they seem at times irreparable.[61] The data is obtained by hackers.[62] It is abused by individual miscreant law enforcement actors who have access.[63] And perhaps foremost of all these, this much personal data in the hands of executive agencies and actors poses the gravest of

[60] Citron, supra note 6, at 50–63 (exploring the harms resulting from governmental amassing of vast reservoirs of data, including control over people's bodies, denial of benefits, stigmatization, chilling of expression, blackmail, and extortion); Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1935 (2013) (underscoring risk of chilling of civil liberties, unequal power, and threat of selective enforcement as a result of government surveillance); see also Danielle Keats Citron & Daniel J. Solove, Privacy Harms, 102 B.U. L. Rev. 793, 830–61 (2022) (exploring physical, economic, reputational, psychological, autonomy, discrimination, and relationship harms as a result of surveillance); Natasha Singer & Brian X. Chen, In a Post-Roe World, the Future of Digital Privacy Looks Even Grimmer, N.Y. Times (June 22, 2023), https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html [https://perma.cc/83HW-NQFH] (discussing how law enforcement acquisition of personal data enables widespread surveillance, including reproductive health tracking that could enable abortion prosecutions).

[61] See, e.g., Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 35, 47–52 (2017); Danielle Keats Citron, A Poor Mother's Right to Privacy: A Review, 98 B.U. L. Rev. 1139, 1142 (2018) (reviewing Khiara M. Bridges, The Poverty of Privacy Rights (2017)); Buolamwini & Friedman, supra note 18; Nicol Turner Lee & Caitlin Chin-Rothmann, Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color, Brookings Inst. (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/QJ2V-C59G].

[62] See, e.g., Josh Fruhlinger, The OPM Hack Explained: Bad Security Practices Meet China's Captain America, CSO (Feb. 12, 2020), https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html [https://perma.cc/3YGE-EBAM]; Kyle Barr, Hackers Infiltrated Multiple U.S. Law Enforcement Data Systems, Report Shows, Gizmodo (May 12, 2022), https://gizmodo.com/hackers-dea-lapsus-internal-databases-u-s-law-enf-1848917172 [https://perma.cc/KJ3D-VF96] (reporting that hackers had accessed sixteen U.S. law enforcement databases).

[63] See, e.g., Police Sometimes Misuse Confidential Work Databases for Personal Gain: AP, CBS News (Sept. 30, 2016, 8:59 AM), https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/ [https://perma.cc/USN7-KWYN] (outlining numerous instances in which police officers used law enforcement databases inappropriately and noting how difficult it is to track the frequency of such abuses); Alina Selyukh, NSA Staff Used Spy Tools on Spouses, Ex-Lovers: Watchdog, Reuters (Sept. 27, 2013, 3:34 PM), https://www.reuters.com/article/idUSBRE98Q14H/ [https://perma.cc/M3C6-8BTN]; see also Neil M. Richards, Why Privacy Matters 147 (2021) ("[R]isks—and abuses—are inevitable, even by otherwise well-meaning agents who zealously pursue their targets . . . ."); Daniel J. Solove, Nothing to Hide: The False Tradeoff Between Privacy and Security 27 (2011).

dangers, from rounding up the unpopular, to widescale violations of individual liberty, to totalitarian government.[64]

Law enforcement agencies acting in coordination with private actors to gather all this information know full well that their conduct is problematic. We know that they know, because they go to great lengths to hide it.[65] Evasion is the name of the game. Private-public contracts require confidentiality, prohibiting policing agencies from breathing a word about the details.[66] Agencies sign memoranda of understanding and contracts with private data purveyors that forbid acknowledging access to and use of data surveillance tools or even testifying about it in court or to other government officials.[67] Agencies engage in "parallel construction,"

[64] For prescient examples, see Bedi & McGrory, infra, as well as that department's other initiative, which uses school and other data to compile a list of kids deemed likely to "fall into a life of crime." Neil Bedi & Kathleen McGrory, Pasco's Sheriff Uses Grades and Abuse Histories to Label Schoolchildren Potential Criminals, Tampa Bay Times (Nov. 19, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/ [https://perma.cc/X23J-JKYV]; see also Ángel Díaz, When Police Surveillance Meets the 'Internet of Things,' Brennan Ctr. for Just. (Dec. 16, 2020), https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things [https://perma.cc/83QH-6EZD] (providing one example of how advances in technology and increased law enforcement acquisition of personal data can add up to near-panopticon levels of government surveillance).

[65] The understanding we have is because of investigative reporters, advocates' research reports, and FOIA litigation. See, e.g., Hemisphere: Law Enforcement's Secret Call Records Deal with AT&T, Elec. Frontier Found., https://www.eff.org/cases/hemisphere [https://perma.cc/L6Z9-NN2H] (last visited May 15, 2024); Gabriella Sanchez & Rachel Levinson-Waldman, Police Social Media Monitoring Chills Activism, Brennan Ctr. for Just. (Nov. 18, 2022), https://www.brennancenter.org/our-work/analysis-opinion/police-social-media-monitoring-chills-activism [https://perma.cc/XEM3-EWZW]; Laura Hecht-Felella, Federal Agencies Are Secretly Buying Consumer Data, Brennan Ctr. for Just. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data [https://perma.cc/H2RU-ER37].

[66] Shenkman et al., supra note 32, at 42 (detailing nondisclosure clauses in government contracts with location data broker Babel Street). Computer scientist Jack Poulson and his team are studying federal procurement records to untangle the complicated arrangements between government agencies and tech companies and subcontractors. Sean Captain, Meet the Ex-Googler Who's Exposing the Tech-Military Industrial Complex, Fast Co. (Oct. 8, 2021), https://www.fastcompany.com/90682901/meet-the-ex-googler-whos-exposing-the-tech-military-industrial-complex [https://perma.cc/3YSW-PCNC].

[67] Sam Adler-Bell, Beware the 'Stingray,' U.S. News & World Rep. (Mar. 13, 2015, 10:45 AM), https://www.usnews.com/opinion/articles/2015/03/13/stingray-lets-police-spy-on-cellphones-and-they-want-to-keep-it-secret [https://perma.cc/9ZP6-DEM5]; John Kelly, Cellphone Data Spying: It's Not Just the NSA, USA Today (Aug. 11, 2015, 11:51 AM), https://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ [https://perma.cc/8AEH-34CB]; Matt Cagle, Dirtbox Over Disneyland? New Docs Reveal Anaheim's Cellular Surveillance Arsenal, ACLU N. Cal. (Jan. 27, 2016), https://www.

meaning they create a basis for a law enforcement action that can be divulged in public filings, while hiding how they really discovered the information.[68] For documents that are likely to end up public, such as government contracts, deceptive language is used to hide the fact that agencies are getting a bespoke product from vendors, and not something that is generally commercially available.[69] In formal legal opinions, agencies are playing fast and loose with their interpretation of *Carpenter*.[70]

Law enforcement sometimes argues that they cannot reveal these techniques lest the people engaging in criminal conduct learn about the countermeasures being used against them, but these arguments strain credulity and undermine basic principles of democratic governance. It is hardly a secret that things like location data are available to law enforcement; those engaging in criminality use the same data themselves.[71] More fundamentally, it deeply misunderstands the role of policing officials and their place in our system of government that they view it appropriate to try to avoid judicial scrutiny and democratically

aclunc.org/blog/dirtbox-over-disneyland-new-docs-reveal-anaheim-s-cellular-surveillance-arsenal [https://perma.cc/83PW-UKEB]; Barry Friedman, Secret Policing, 2016 U. Chi. Legal F. 99, 103–04.

[68] Trevor Aaronson, Welcome to Law Enforcement's "Dark Side": Secret Evidence, Illegal Searches, and Dubious Traffic Stops, The Intercept (Jan. 9, 2018, 9:57 AM), https://theintercept.com/2018/01/09/dark-side-fbi-dea-illegal-searches-secret-evidence/ [https://perma.cc/C44Q-G9GN]; Kenneth Lipp, AT&T Is Spying on Americans for Profit, Daily Beast (Apr. 13, 2017, 2:36 PM), https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit [https://perma.cc/C2ME-CK8T].

[69] Shenkman et al., supra note 32, at 19–21.

[70] ODNI Report, supra note 23, at 13, 20; see also Byron Tau & Michelle Hackman, Federal Agencies Use Cellphone Location Data for Immigration Enforcement, Wall St. J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 [https://perma.cc/J44R-N3YR] ("[T]he federal government has essentially found a [way around *Carpenter*] by purchasing location data used by marketing firms rather than going to court on a case-by-case basis."); Charlie Savage, Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says, N.Y. Times (Jan. 25, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html [https://perma.cc/79SU-JY64].

[71] Indeed, fraudsters' purchase of data broker dossiers is why ChoicePoint settled with the FTC to strengthen its security practices in 2009. Press Release, Fed. Trade Comm'n, Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months (Oct. 19, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers-personal-data-left-key-electronic [https://perma.cc/YC9P-NVPA].

accountable governance.[72] As we are about to see, that has been the consistent view of Congress since the start of the digital information revolution.

II. CONGRESS'S CONSISTENT REJECTION OF INDISCRIMINATE DATA COLLECTION AND INSISTENCE ON REGULATION

This Part documents how, from the 1960s to the present, when forced to address practices of indiscriminate data collection, Congress routinely shut them down or imposed significant rule-of-law-based requisites and constraints. To be clear, Congress not infrequently ducked these issues when presented with them. That is because, as this Part also shows, law enforcement is quick to argue necessity and plead peril when faced with any regulation, and members of Congress are loath to take them on about this, even when the claims are not sufficiently substantiated or when regulations could be drafted with some precision to avoid the problem. Part III explores this dynamic at greater length, offering suggestions about how to overcome it.

When Congress has had no choice but to act, however, it has changed the status quo. Typically, it banned altogether collecting data on American individuals for whom there was no suspicion of unlawful

[72] This particularly is a concern because so much technology developed for use in national security has been imported into domestic law enforcement. See, e.g., Spencer Ackerman, Your Local Cops Now Use Iraq's Iris Scanners, Wired (Dec. 20, 2010, 10:19 AM), https://www.wired.com/2010/12/your-local-cops-now-use-iraqs-iris-scanners/ [https://perma.cc/SAR7-6A8H] (describing how police use iris scanners developed for use in Iraq and Afghanistan conflicts); Matthew Guariglia, Stop Military Surveillance Drones from Coming Home, Elec. Frontier Found. (Sept. 21, 2021), https://www.eff.org/deeplinks/2021/09/stop-military-surveillance-drones-coming-home [https://perma.cc/BW7D-5FT6] (expressing concern about military drones in domestic law enforcement); see also Jonathan Hafetz, Homeland Security's Fusion Centers Show the Dangers of Mission Creep, The Hill (Mar. 19, 2023, 12:00 PM), https://thehill.com/opinion/national-security/3900077-homeland-securitys-fusion-centers-show-the-dangers-of-mission-creep/ [https://perma.cc/5U57-G8L4] (describing how fusion centers created to fight terrorism now are being used for all crimes and hazards). See generally Tom Schuba & Frank Main, CPD Launched Secret Drone Program with Off-the-Books Cash, Chi. Sun-Times (May 12, 2021, 12:02 PM), https://chicago.suntimes.com/city-hall/2021/5/11/22425299/cpd-chicago-police-drone-secret-emails-hack-lori-lightfoot-dodsecrets-city-hall [https://perma.cc/J2XW-YNV7] (describing the Chicago Police Department's pilot drone surveillance program); Sebastian Cahill, Police Use of High Tech Drones Is on the Rise, and Regulations Aren't Keeping Up with Them, Bus. Insider (July 6, 2023, 10:07 PM), https://www.businessinsider.com/police-department-drones-local-regulations-baltimore-laws-technology-robots-2023-7 [https://perma.cc/9U3E-SS3V] (noting that in 2021, only fifteen states required a warrant for law enforcement drone use).

conduct. When collection was allowed, it was carefully regulated along lines that echoed constitutional and rule-of-law norms, which members of Congress brought up repeatedly. There was widespread agreement that domestic law enforcement agencies simply should not be amassing or accessing digital dossiers on American citizens and other individual residents in the country without legislative authorization and appropriate safeguards. This Part describes these critical moments in national history, identifying the requisites Congress demanded and the constraints it insisted upon before indiscriminate bulk data collection could continue.

Before we begin, a word on terminology. Congressional legislation in this area often distinguishes between individuals believed to be protected by the United States Constitution under governing Supreme Court precedent, and those who are not.[73] At times, we use the typical statutory language—"United States persons"—to refer to those so protected, which includes all American citizens and any other person resident in the United States. At other times, though, for simplicity, we refer to "Americans." We distinguish those who enjoy constitutional protections from those who do not, referring to the latter individuals as "foreigners abroad" or simply "foreigners." Despite the clarity of the distinction, the lines themselves have been contested over time.[74]

A. Early Concerns About Government Databases: Enacting the Privacy Act

In the early 1970s, a bipartisan congressional consensus emerged that government collection of computerized "dossiers"—even of the most basic information needed to govern—posed unique dangers that required transparency, congressional authorization, and attendant safeguards.[75] In

[73] The case typically cited for this proposition is *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), though it alone is a rough analogy at best. *Verdugo-Urquidez* involved the arrest of a foreigner abroad for trial in the United States. Id. at 262.

[74] See generally Scott Bomboy, The Birthright Citizenship Debate Returns for 2020 Election, Nat'l Const. Ctr. (Aug. 14, 2020), https://constitutioncenter.org/blog/the-birthright-citizenship-debate-returns-for-2020-election [https://perma.cc/95KW-ASG5] (discussing debates over whether a person should automatically qualify for American citizenship based on their location of birth).

[75] Privacy: The Collection, Use, and Computerization of Personal Data: Joint Hearings on S. 3418, S. 3633, S. 3116, S. 2810, and S. 2542 Before the Ad Hoc Subcomm. on Priv. & Info. Sys. of the S. Comm. on Gov't Operations and the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary, 93d Cong. 1–3, 52 (1974) [hereinafter Senate Privacy Hearing I] (statement of Sen. Sam J. Ervin and statement of Sen. Jacob Javits).

extensive hearings before joint House and Senate committees investigating the "Collection, Use, and Computerization of Personal Data," lawmakers repeatedly expressed serious concerns about the threats posed by computerization of personal data. Republican Senator Jacob Javits of New York opened the hearings, highlighting the "new menaces of computer data banks and indiscriminate government and private sector dossiers."[76] Senator Sam J. Ervin, a southern Democrat and widely acknowledged constitutional expert, who served as Chair of the Judiciary's Subcommittee on Constitutional Rights, shared the sentiment: "Privacy, like many of the other attributes of freedom, can be easiest appreciated when it no longer exists. . . . We should not have to conjure up 1984 or Russian-style totalitarianism to justify protecting our liberties against Government encroachment."[77] Democratic Representative Don Edwards of California worried that "agencies collect a little more information today, a little more information tomorrow, and pretty soon there is a complete dossier on every individual in this country."[78] These concerns were echoed by conservative Republican Senator Barry Goldwater of Arizona, his party's presidential candidate in 1964, who asked: "Where will it end? . . . Will we permit all computerized systems to interlink nationwide so that every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution?"[79]

Lawmakers recognized two distinct types of harms of computerized dossiers, which would echo in congressional debates in years to come: threats to individuals, and those to society. Individual interests threatened included privacy, reputation, livelihood, and liberty.[80] Connecticut Senator Abraham Ribicoff drew attention to the fact that government files contained personal information of "a most personal nature"—some "outdated and incorrect" and some accurate—that would be used to make decisions about people's lives.[81] People could be denied housing,

[76] Id. at 52 (statement of Sen. Jacob Javits).
[77] Id. at app. 352 (remarks by Sen. Sam J. Ervin on introducing S. 3418).
[78] Id. at app. 1676.
[79] 120 Cong. Rec. 36904 (1974) (statement of Sen. Barry Goldwater).
[80] Senate Privacy Hearing I, supra note 75, at 1609–10, 1613 (statement of Sen. Sam J. Ervin); see also id. at 1696 (including Jerome B. Wiesner, The Information Revolution—and the Bill of Rights, 5 Law & Comput. Tech. 20 (1972)) ("Our task is to achieve a proper balance between the ability to cope with individual threats to the society and its capability to abridge the freedom and happiness of its members.").
[81] 120 Cong. Rec. 36916 (1974) (statement of Sen. Abraham Ribicoff).

employment, and educational opportunities.[82] Senator Ervin noted that "computerized dossiers" had operated as blacklists, preventing people from bidding on government contracts or obtaining licenses.[83] But the power accruing to government and society from the possession of vast quantities of personal information was deemed even more perilous.[84] Representative Edwards warned that the "day of big brother and constant surveillance is already upon us" as "law enforcement agencies, military agencies, or other agencies of authority are given unfettered access to these records."[85] Senator Barry Goldwater presaged the Pentagon's "Total Information Awareness" program (quickly shut down by Congress in 2003) when he said total integration of public and private databases could facilitate authoritarian impulses because "total control requires total information."[86] Indiana's Democratic Senator Birch Bayh described a "dictatorship of dossiers" to which everyone is subject, "[r]ich or poor, male or female, right or left in political ideology, whatever one's cultural style or religious views."[87]

Lawmakers were particularly alarmed that agencies were building databases of personal data without legislative permission—a consistent theme throughout the hearings.[88] Senator Sam J. Ervin said he was "disturbed by the fact that, by and large, data banks *lack express congressional authorization*. Only about one-sixth of the reported [858 federal] data banks [with 1.25 billion records on people] could cite a specific statute which explicitly authorizes the system."[89] He underscored that "[o]nce collected and computerized, personal data . . . takes on a life of its own," is "aggregated into a 'data profile' of the individual subject," and shared among agencies, *even though no statute permitted or required*

[82] Id. at app. 1676.

[83] Id. at 4; Sam J. Ervin, Jr., The First Amendment: A Living Thought in the Computer Age, 4 Colum. Hum. Rts. Rev. 13, 19, 29 (1972).

[84] Senate Privacy Hearing I, supra note 75, at app. 1676.

[85] Id. (statement of Rep. Don Edwards).

[86] Id. at app. 1738–39 (testimony of Sen. Barry Goldwater).

[87] Id. at 18 (statement of Sen. Birch Bayh).

[88] In addition to Ervin's remarks, see, for example, id. at 7, app. 2252 (statement of Sen. Abraham Ribicoff) ("Only 10 percent [of those databanks] have been specifically authorized by statute."). Representative Edward Koch argued that legislation was needed to "make clear the source and limitations" of governmental authority to handle personal data. Id. at 21 (statement of Rep. Edward Koch).

[89] Id. at 4 (statement of Sen. Sam J. Ervin) (emphasis added).

such sharing.[90] The solution to a "nightmare of secret data banks surreptitiously recording data about innocent Americans," Ervin insisted, was a "legislative requirement that every Federal data bank be authorized by an explicit congressional mandate."[91]

Congress called for the adoption of a set of "fair information practices" to safeguard against secret, "indiscriminate," and unaccountable databases of personal data.[92] For Senator Ervin, transparency was the essential first step given the "[w]idespread reluctance on the part of many of the agencies to disclose to the Congress just how many and what kinds of data systems these agencies have and how they use them."[93] This would allow Congress and private individuals to evaluate and police the operation of these systems.[94] Representative Barry Goldwater, Jr. insisted on the need to limit the use of information to the initial purpose for which it was collected.[95] He objected to government files "float[ing] from agency to agency."[96] His father, Senator Goldwater, argued for what today we call "minimization": that computers should be "programmed to erase unwanted" details of people's past, including health, education, "telephone calls," "books borrowed," and "family relationships."[97]

The outcome of these discussions was a comprehensive set of rules regarding the government's collection of private data—the Privacy Act

[90] Id. at 3, app. 2253 (noting that "60% of the data banks regularly share their files . . . with other agencies" without statutory approval); see also 120 Cong. Rec. S1296 (daily ed. Feb. 5, 1974) (statement of Sen. Sam J. Ervin) (arguing that criminal justice databases needed clear statutory authorization).

[91] Id. at 4 (statement of Sen. Sam J. Ervin).

[92] An advisory committee created by the Secretary of Health, Education, and Welfare, chaired by Willis Ware, issued a report in July 1973 laying out a code of "fair information practices"—members of the advisory committee testified before the House and Senate in 1973 and 1974. U.S. Dep't of Health, Educ. & Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, at xx (1973).

[93] Senate Privacy Hearing I, supra note 75, at 4 (statement of Sen. Sam J. Ervin); see also id. at 40 (statement of Hon. Elliot L. Richardson) (suggesting that legislation should clearly apply to all federal agencies).

[94] Id. at 4 (statement of Sen. Sam J. Ervin).

[95] Id. at app. 1675 ("[C]itizens give [us] personal information . . . on a confidential basis and for a specific purpose. Americans deserve the assurance that this information will not be used for any other purpose in the future.").

[96] Id.

[97] Criminal Justice Databanks—1974: Hearings Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary, 93d Cong. 140–41 (1974) (statement of Sen. Barry Goldwater) (noting that statistical information in government and private databases could be purchased, matched to individuals, and used to "manipulate . . . social conduct").

of 1974. The Privacy Act incorporated the fair information practices described above. *Transparency* is achieved through the requirement that federal agencies publish notices about the "existence and character" of "systems of records" that can be accessed via personal identification.[98] The Privacy Act's solution to the authorization problem was to grant general permission to agencies to collect information so long as it "is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[99] Information sharing outside the agency to any other person *or* agency is permissible if doing so would be "compatible with the purpose for which [the personal information] was collected."[100] The "civil or criminal law enforcement" exception allows an agency to obtain a record "if the activity is authorized by law" and the "head of the agency or instrumentality has made a written request to the agency . . . specifying the particular portion desired and the law enforcement activity for which the record is sought."[101] And there are a host of *safeguards*, including a strict ban on the collection of information solely about First Amendment activities,[102] and individual recourse to ensure individual access to records and checks to ensure the accuracy of information.[103]

B. The Law Enforcement Exemption and Legislation That Never Came to Be

Yet, despite all of the concern over widespread collection and storage of personal data, the seeds of today's trouble were planted with specific law enforcement exemptions written into the Privacy Act.[104] Under the Privacy Act, agencies that enforce criminal law—such as the Federal

[98] 5 U.S.C. § 552a(e)(3)–(4).

[99] Id. § 552a(e).

[100] Id. § 552a(b)(3); Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law 96–97 (1996) ("The principle of compatibility requires a significant degree of convergence and a concrete relationship between the purpose for which the information was gathered and its application.").

[101] 5 U.S.C. § 552a(b)(7). There is also a general exemption provision discussed infra note 104 and accompanying text.

[102] 5 U.S.C. § 552a(e)(7).

[103] Id. § 552a(d); see also The Privacy Act of 1974, Elec. Priv. Info. Ctr., https://epic.org/the-privacy-act-of-1974/ [https://perma.cc/EX3Z-8G3U] (last visited Aug. 25, 2024) (providing overview of the provisions of the Privacy Act of 1974).

[104] 5 U.S.C. § 552a(j) (general exemptions via the promulgation of rules); id. § 552a(k) (specific exemptions via the adoption of rules related to investigatory materials for law enforcement purposes).

Bureau of Investigation ("FBI"), the Department of Justice ("DOJ"), and the Internal Revenue Service ("IRS")—may promulgate rules that exempt certain records in "systems of records" from the law's requirements.[105] When an agency exercises its exemption power, claims that individuals "may once have had are extinguished."[106]

Lest the law enforcement exemption in the Privacy Act seem to end our argument before it even gets going, note three important things: First, the exemption was included by members who believed that the 94th Congress would pass additional legislation specifically governing criminal justice databases. In 1973 and 1974, Congress held hearings about the FBI's National Crime Information Center ("NCIC"), a database that linked criminal justice records to computers in federal, state, and local law enforcement agencies.[107] Second, these law enforcement databases at the time *did not* amass records indiscriminately, but were based on suspicion involving "wanted criminals, . . . stolen cars, firearms, securities, and other stolen property."[108] Third, quite obviously the volume of data and artificial intelligence tools available to aggregate and analyze it simply were unavailable at the time.

Concern about criminal databases was often expressed in constitutional terms. Members of Congress argued that restrictions on NCIC were necessary to "secure the constitutional rights guaranteed by" the First, Fourth, Fifth, Sixth, Ninth, and Fourteenth Amendments.[109] They maintained that the NCIC database "stripped [Americans] of [their] privacy" and gave government too much power: "The Bill of Rights then becomes just so many words."[110]

[105] Id. § 552a(j). In his congressional testimony, former Attorney General Elliot Richardson stated: "I do not believe that the legislation itself should create exemptions . . . . The tendency will exist for agencies to construe any exemption more broadly than it is intended to apply." Senate Privacy Hearing I, supra note 75, at 43 (statement of Elliot Richardson); see, e.g., Carp v. IRS, No. 00-cv-05992, 2002 WL 443478, at *6 (D.N.J. Jan. 28, 2003) (holding that the Criminal Investigative Division of IRS was covered by exemption); Schulze v. FBI, No. 05-cv-00180, 2010 WL 2902518, at *15 (E.D. Cal. July 22, 2010) (finding that the (j)(2) "exemption is both categorical and enduring").

[106] Williams v. Farrior, 334 F. Supp. 2d 898, 905 (E.D. Va. 2004).

[107] Senate Privacy Hearing I, supra note 75, at app. 1677–78; Aryeh Neier, Dossier: The Secret Files They Keep on You 100–01 (1975).

[108] Neier, supra note 107, at 100.

[109] S. 2963, 93d Cong. § 101 (1974).

[110] Criminal Justice Databanks—1974: Hearings Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary, supra note 97, at 17 (statement of Sen. Sam J. Ervin) ("Congress must act before those new systems are developed. . . . The peculiarity of those new complex

Unfortunately, though—and underscoring a consistent theme of this history—bipartisan efforts to pass legislation regulating criminal justice databases petered out due to strong and sustained opposition by law enforcement agencies.[111] The Treasury Department, Securities and Exchange Commission, Federal Trade Commission, and Department of Justice insisted that virtually *any* restriction on criminal justice databases would make it difficult to fight illegal activity.[112] Deputy Attorney General Harold R. Tyler, Jr. opposed legislation that forbade "uses" of records that Congress had not explicitly authorized. "Sometimes a scrap of information, as innocent as the report that somebody has entered a telephone booth, proves to be the most important."[113]

Although law enforcement prevailed in its efforts to fend off regulation, a 1977 report by the Privacy Protection Study Commission, mandated by the Privacy Act, highlighted ongoing fears about criminal databases. Nothing was done about them because (in Congress-speak) their regulation turned out to be more complicated than expected.[114] Still, there was worry about the "continuing growth in the government's appetite for information about individuals," the lack of mechanisms to ask whether a record-keeping system "should exist at all," and the "gradual erosion of individual liberties through the automation, integration, and interconnection of many small separate record-keeping systems, each of which alone may seem innocuous, even benevolent."[115] The Commission was particularly concerned with the Privacy Act's failure to protect privacy in "sophisticated criminal justice information systems" shared

technologies is that once they go into operation, it is too late to correct our mistakes or supply our oversight.").

[111] Criminal Justice Information and Protection of Privacy Act of 1975: Hearings Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary, 94th Cong. 149, 156 (1975) [hereinafter Criminal Justice Information and Protection of Privacy Act Hearing].

[112] Senate Privacy Hearing I, supra note 75, at app. 460–62, 474–76, 478–84 (noting objections by DOJ, Securities and Exchange Commission, Treasury Department, and FTC to Ervin's proposed privacy bill).

[113] Criminal Justice Information and Protection of Privacy Act Hearing, supra note 111, at 213 (statement of Deputy Att'y Gen. Harold Tyler, Jr.). Tyler explained that the DOJ worried about limiting sharing of information with other agencies unless an "articulable fact standard" is met. Id. at 212.

[114] Donald A. Marchand, The Politics of Privacy, Computers, and Criminal Justice Records: Controlling the Social Costs of Technological Change 189–202 (1980).

[115] Priv. Prot. Study Comm'n, The Privacy Act of 1974: An Assessment 108 (1977). The members of the Commission included Dr. Willis H. Ware of the RAND Corporation, who served as Vice Chairman; Congressman Barry M. Goldwater, Jr. of Arizona; and Congressman Edward I. Koch of New York. Id. at iii.

with state and local law enforcement agencies.[116] The "unrestricted information flows between law enforcement and investigative agencies at all levels of government" are "amenable to abuse" and still lack "oversight mechanisms to assure their accountability."[117] In its view, law enforcement only should collect personal data if it is "authorized by a statute that details the purpose for the reporting and the standards of relevance for any information collected."[118]

C. The Church Committee's Enduring Framework for Domestic and Foreign Surveillance

The failure to regulate law enforcement's data collection practices hardly was over though: just as the Privacy Act was being enacted, concerns about indiscriminate data collection lacking congressional authorization or oversight surfaced in response to the FBI's surveillance of activists, protestors, and journalists in the 1960s and 1970s, as well as the National Security Agency's ("NSA") partnership with corporate America in enabling the bulk collection of telegrams going in and out of the United States. Although the Privacy Act exemptions of law enforcement stood, the 1970s revelations led to a critical framework for law enforcement data collection about United States persons that persists (in changed form) to this day.

1. Ending Indiscriminate Domestic Spying

On December 22, 1974, the *New York Times* exposed details of the CIA's years-long illegal spying campaign against thousands of American antiwar activists.[119] On the heels of Watergate hearings and President Nixon's resignation, the article spurred Senate Majority Leader Mike Mansfield to appoint Democratic Senator Frank Church to lead a Senate Select Intelligence Committee ("Church Committee") to investigate law enforcers' and intelligence agencies' illegal spying on Americans.[120] Republican Senator John Tower of Texas served as co-chair.[121] Senators

[116] Id. at 109.
[117] Id.
[118] Sarah P. Collins, Cong. Rsch. Serv., Rep. No. 79-236, The Privacy Protection Study Commission: Background and Recommendations 52 (Oct. 31, 1979).
[119] James Risen with Thomas Risen, The Last Honest Man: The CIA, the FBI, and the Kennedys, and One Senator's Fight to Save Democracy 159–60 (2023).
[120] Id. at 118–19.
[121] Id. at 172.

Church and Tower understood that the "United States had created a national security state with virtually no debate" since World War II and now the U.S. public demanded it.[122]

The Church Committee uncovered vast networks of spying and illegal operations at the FBI, often aimed at Americans suspected of no criminal activity who were engaged in constitutionally protected activities. From 1956 to 1971, FBI Director J. Edgar Hoover approved a counterintelligence program code-named COINTELPRO. COINTELPRO was designed to target the "Communist threat," but quickly moved far beyond communist-affiliated groups to any domestic dissenters, from members of groups as varied as the civil rights movement, women's liberation movements, and white hate groups.[123] Mission creep was regrettably routine: the Church Committee found "a consistent pattern in which programs initiated with limited goals, such as preventing criminal violence or identifying foreign spies, were expanded to what witnesses characterized as 'vacuum cleaners,' sweeping in information about lawful activities of American citizens."[124]

Of particular concern to the Church Committee was the indiscriminate nature of the surveillance. The FBI subjected hundreds of thousands of Americans to warrantless wiretaps, microphone bugs, secret mail opening, and break-ins due to their membership in disfavored political groups.[125] Under the auspices of COINTELPRO and other surveillance programs, the FBI amassed files on more than one million Americans.[126] This was "secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts."[127] FBI's investigations went on "without stop, and without regard to whether or not information ha[d] been collected which is of any use whatsoever to a purpose of looking for a criminal violation, or for dealing with any purpose concerning which one would have thought the Federal

[122] Id. at 179.

[123] S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities, Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755, bk. II, at 65–66 (1976) (identifying a communist threat); Loch K. Johnson, A Season of Inquiry Revisited: The Church Committee Confronts America's Spy Agencies 126–27 (2d ed. 2015).

[124] S. Rep. No. 94-755, bk. II, at 3–4 (1976).

[125] Id. at 5.

[126] Loch K. Johnson, Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee, 64 Pub. Admin. Rev. 3, 6 (2004).

[127] S. Rep. No. 94-755, bk. II, at 5 (1976).

Government ought to be collecting information."[128] Senator Philip Hart underscored the fact that the FBI's activities were not "in pursuit of any crime at all."[129]

For the Church Committee, the answer to these sorts of indiscriminate domestic intelligence gathering practices was "stark and simple": "the obvious solution is to prohibit them altogether."[130] Senator Walter Mondale of Wisconsin, who led the Select Committee's investigation into COINTELPRO, noted, "If there is one lesson that our Committee felt above all must be learned from our study of the abuses . . . it has been the crucial necessity of establishing a system of congressional oversight."[131] Mondale pressed back on Attorney General Edward Levi's testimony that the FBI had sufficient general authority to act against a group or individual, finding that the Attorney General "seemed to have forgotten that the job of the FBI was to focus on actual or suspected violations of the law, not just the expression of ideas."[132]

2. Foreign Intelligence Gathering

What Congress ultimately concluded about indiscriminate domestic spying largely has to be understood in the context of what it did about foreign intelligence gathering. The Church Committee also laid bare a decades-long secret spying program—called Operation Shamrock—run by the NSA for the ostensible purpose of securing the nation from *foreign* threats.[133] From September 1, 1945, to May 15, 1975, in response to government entreaties, and sidestepping concerns about legality, RCA Global Corporation, Western Union Telegraph, and ITT World Communications provided intelligence agencies with copies of all messages leaving and entering the United States.[134] NSA computers were "fed every single cable sent overseas by Americans," and intelligence

[128] Intelligence Activities—Federal Bureau of Investigation: Hearings Before the S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities, 94th Cong. 5 (1975) (statement of F.A.O. Schwarz, Jr., Chief Counsel, S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities).

[129] Id. at 74 (statement of Sen. Philip Hart).

[130] S. Rep. No. 94-755, bk. II, at 292 (1976).

[131] Johnson, supra note 126, at 10.

[132] Id. at 8.

[133] S. Rep. No. 94-755, bk. II, at 104, 169 (1976).

[134] James Bamford, The Puzzle Palace: A Report on America's Most Secret Agency 384–85 (1983). The NSA took over the program in 1952 when the agency was created by a secret presidential memorandum. Id. at 386.

gleaned from these telegrams was shared with domestic law enforcement agencies, including the FBI.[135]

The Church Committee's public hearings about the bulk telegram program revealed congressional fury about indiscriminate and bulk data collection on innocent Americans and a deeply felt need for regulation.[136] In a remarkable, if historically all-too-typical exchange, Senator Walter Mondale repeatedly asked the NSA's Deputy Director, Benson Buffham, if, at any point, he was concerned about the program's legality and propriety; after several non-answers, Buffham responded: "We didn't consider it at the time, no."[137] Senator Richard Schweiker of Pennsylvania "could not condone" such government "snooping" and said that "to be silent would be to give consent."[138] The familiar twin harms were apparent to Senator Church: when government has access to technology that monitors all communications, not only do Americans lose their privacy, but they risk falling prey to a dictator who would use that capability to accomplish "total tyranny."[139]

The Church Committee report condemned the warrantless bulk collection of Americans' private information, declaring that it should end. To dispel any ambiguity, the report explained that intelligence agencies should not undertake any "operation such as SHAMROCK."[140] It did not matter if the ultimate concern was foreign intelligence; what mattered was that Americans' information was at stake. The Church Committee's report stated that the "NSA should have no greater latitude to monitor the communications of Americans than any other intelligence agency."[141]

The Church Committee's work culminated in the passage of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), which underscored the distinction between collecting "United States persons" information and that of foreign powers, and provided a statutory framework for electronic surveillance conducted in the United States for

[135] Johnson, supra note 126, at 227; Bamford, supra note 134, at 405.

[136] Bamford, supra note 134, at 477.

[137] Johnson, supra note 126, at 9.

[138] Intelligence Activities—The National Security Agency and Fourth Amendment Rights: Hearings Before the S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities, 94th Cong. 64 (1975).

[139] Meet the Press, The Intelligence Gathering Debate, YouTube (Jan. 23, 2014), https://www.youtube.com/watch?v=YAG1N4a84Dk [https://perma.cc/S6RY-N8FU] (NBC television broadcast interview with Senator Frank Church on Aug. 17, 1975).

[140] S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities, Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755, bk. II, at 310 (1976).

[141] Id. at 309.

foreign intelligence purposes.[142] Under FISA, *only* "foreign power[s]" and "agent[s] of a foreign power" could be targeted for electronic surveillance under the law.[143] Electronic surveillance of Americans for criminal law enforcement purposes would continue to be governed by the tight strictures of the Wiretap Act of 1968, which required heightened showings of probable cause for warrants and imposed strict minimization requirements.[144]

But even FISA itself did not allow for indiscriminate data collection of anyone, and it contained familiar regulatory controls over the actions of intelligence agencies. It established the Foreign Intelligence Surveillance Court ("FISC" or "FISA Court") to review government requests for electronic surveillance.[145] Any electronic surveillance in the United States had to be approved by the FISC, or (in an emergency) the Attorney General—and still an application had to be made to the FISC within 72 hours.[146] The government agency's FISA application would have to demonstrate probable cause to believe that the "target of the electronic surveillance is a foreign power or an agent of a foreign power," that "a significant purpose of the surveillance is to obtain foreign intelligence information," and that appropriate "minimization procedures" are in place.[147] Each application had to be approved and signed by the Attorney General.[148] The NSA was "required to make every practicable effort to eliminate or minimize the extent to which the communications of Americans are intercepted, selected, or monitored."[149] And incidental monitoring of domestic communications could not be disseminated unless they provided "evidence of hostile foreign intelligence" activity, a felony,

[142] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783. Congress acted in the shadow of the 1972 *Keith* decision, *United States v. U.S. Dist. Ct.*, 407 U.S. 297 (1972), which brought electronic surveillance conducted in the name of national security "into the scope of the fourth amendment, and strongly suggested that Congress regulate such surveillance." Foreign Intelligence Surveillance Act of 1978, S. Rep. No. 95-701, at 91 (1978), *reprinted in* Legislative History of the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, at 4042, https://irp.fas.org/agency/doj/fisa/wallop.pdf [https://perma.cc/N2J4-SZAZ] (additional views of Sen. Malcolm Wallop).

[143] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 104(a)(4)(A), 92 Stat. 1783, 1789 (codified at 50 U.S.C. § 1804(a)(3)(A)).

[144] 18 U.S.C. § 2518.

[145] 50 U.S.C. § 1801; id. § 1803(e).

[146] Id. § 1805(f).

[147] Id. § 1804(a)(3)(A), (a)(6)(B), (a)(4).

[148] Id. § 1804(a).

[149] S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities, Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755, bk. II, at 309 (1976).

or a threat of "serious bodily harm."[150] The penalty for a single violation was five years in prison.[151]

In short, the indiscriminate collection of Americans' data was not to happen at all, even for national security purposes. And when Americans' data was collected, that was to occur under a familiar constitutional regime that involved judges, warrants, a probable cause predicate, and minimization of unnecessary data.

D. Condemnation of the Unauthorized Terrorist Surveillance Program and Implementation of Safeguards

And there matters largely rested—a defining resolution to the question of indiscriminate data collection, in bulk or otherwise—for a generation or more, until the attacks on 9/11.[152] Vice President Dick Cheney, who served in the Ford White House during the Church Committee hearings,

[150] Id.

[151] 50 U.S.C. § 1809(c). It also was the case that the courts and the Department of Justice worked to prevent FISA from being used to circumvent the Fourth Amendment by separating intelligence and criminal investigation efforts, in what came to be known as "The Wall." Barry Friedman, Unwarranted: Policing Without Permission 290 (2017). After 9/11, it was believed The Wall partially was responsible for the terrorist attacks of that day succeeding, and it was dismantled. Id. at 290–91. One of us has argued The Wall itself always was ill-advised, but the correct approach was steadfast protection of Fourth Amendment rights of all U.S. persons. Id. at 291; see also id. at 305–06 (arguing collection of data may be permitted on a nondiscriminatory basis if legislatively authorized, but searches of that data require a warrant).

[152] "Largely" may be the key word here. All was not necessarily rosy between 1978 and 2001. For example, from 1983 to 1985 the FBI investigated the Committee in Solidarity with the People of El Salvador ("CISPES") in violation of the restrictions on domestic spying, which led to a congressional investigation. See S. Select Comm. on Intel., 101st Cong., Rep. on the FBI and CISPES 103 (Comm. Print 1989) (concluding that the FBI's investigation, while an "aberration," resulted in an unjustified investigation of political activities that threatened the protection of constitutional rights). In part, the problem during this era was that although FISA's restrictions on intelligence gathering against U.S. persons held firm, the rules for domestic law enforcement were a function of Attorney General guidelines, not congressional statutes. See id. at 16–17 (describing how the FBI sought approval from DOJ under the previously issued "Levi guidelines"; DOJ attorneys approved the ongoing CISPES investigation twice, but found it unjustified at the third review, after which the FBI immediately shut down the investigation). Because these provisions did not have the force of law, they were eroded by subsequent administrations even prior to 9/11. See generally Off. of the Inspector Gen., U.S. Dep't of Just., The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines 29–61 (Sept. 2005), https://oig.justice.gov/sites/default/files/legacy/special/0509/final.pdf [https://perma.cc/6895-9EZE] (detailing changes to the Levi guidelines, including in 1983 and 2001 that lowered the standard for initiating investigations).

viewed FISA with disdain.[153] In the weeks after September 11, 2001, he blamed FISA for the failure to prevent the terrorist attacks and pressed for intelligence efforts that would do an end run around FISA.[154] He succeeded.

On October 4, 2001, President George W. Bush issued a top-secret executive order to the Secretary of Defense about a program code-named Stellar Wind, which authorized two surveillance programs of dubious legality and constitutionality.[155] The first allowed the NSA to access phone calls and emails without a warrant so long as one party was known to be outside the United States and "probable cause existed to believe one of the communicants was engaged in international terrorism."[156] The second authorized bulk collection of *all* telephone and email metadata, including that of Americans.[157] This was accomplished by a secret order that AT&T clone and route all communications, not just its own but also those that traveled over its fiber-optic cables, to the NSA.[158] The system allowed the NSA to engage in "vacuum-cleaner surveillance of all the data crossing the Internet—whether that be people's email, Web surfing, or any other data."[159] The system was "not limited to international traffic but included all domestic U.S. communications."[160] General Michael

[153] Risen with Risen, supra note 119, at 401.

[154] Id. at 401–02; see Eric Lichtblau, Bush's Law: The Remaking of American Justice 152, 154 (2008).

[155] The public learned about the President's secret program in dribs and drabs. A comprehensive OIG report was prepared in 2009 and delivered to congressional oversight committees. 3 Offs. of Inspectors Gen., U.S. Dep't of Def., U.S. Dep't of Just., Cent. Intel. Agency, Nat'l Sec. Agency & Off. of the Dir. of Nat'l Intel., A Review of the Department of Justice's Involvement with the President's Surveillance Program, Annex to the Report on the President's Surveillance Program 3 (July 10, 2009) [hereinafter 2009 OIG Report], https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf [https://perma.cc/XY7Y-3A4F]. That report was only disclosed to the public in April 2015. Press Release, Off. of the Inspector Gen., U.S. Dep't of Just., DOJ OIG Announces the Release of a Further-Declassified Version of Its 2009 Report on the President's Surveillance Program (Sept. 21, 2015), https://oig.justice.gov/news/doj-oig-announces-release-further-declassified-version-its-2009-report-presidents-surveillance [https://perma.cc/K6ES-JYWA]. We rely on the report's description here for clarity but note that Congress and the public did not appreciate the depth of what was going on in a meaningful way in 2005 and 2006. Id.

[156] 2009 OIG Report, supra note 155, at 29.

[157] Id. at 1.

[158] James Bamford, The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America 188, 190–91 (2008). AT&T also created secret rooms in its facilities to be supervised by the NSA. Id. at 190–91.

[159] Id. at 191.

[160] Id. at 194–95.

Hayden, NSA Director, understood that "[n]either of these would follow the procedures of . . . FISA . . . as the act was then understood and certainly as it was then implemented."[161] Secret memoranda provided the authority for these actions.[162]

When news of the bulk electronic surveillance program broke in December 2005, the outcry of federal lawmakers was loud and swift.[163] At a January 2006 Senate Judiciary Committee hearing, Senator Arlen Specter, the committee's chair, expressed frustration: In allowing the NSA to conduct "wiretaps on Americans' international communications without a court warrant," the operation "violate[d] FISA—there's no doubt about that."[164] Senator Richard Durbin expressed dismay that the Administration was "comb[ing] through thousands of ordinary Americans' e-mails and phone calls."[165] Presaging what was to come, Republican Senator Mike DeWine of Ohio noted that "what is not debatable is that both from a constitutional as well as from a policy point of view, the . . . country would be stronger" if the Administration had "come to the Congress for such specific statutory authorization."[166]

Amidst strong pushback from Congress and the public, President Bush ended the bulk electronic surveillance program in January 2007.[167] Jack Goldsmith—who, when he became head of the Office of Legal Counsel in 2003, blew the whistle within the Administration about the dubious legality of the programs—shared the White House's concerns that FISA was overly restrictive given the way that packet-switching internet

[161] Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror 67 (2016).

[162] Id. at 67–68.

[163] James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. Times (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/6ZH8-WQTS].

[164] Eric Lichtblau, Senate Panel Rebuffed on Documents on U.S. Spying, N.Y. Times (Feb. 2, 2006), https://www.nytimes.com/2006/02/02/politics/senate-panel-rebuffed-on-documents-on-us-spying.html [https://perma.cc/JF8N-BGRB].

[165] Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the S. Comm. on the Judiciary, 109th Cong. 71 (2006), https://www.govinfo.gov/content/pkg/CHRG-109shrg27443/pdf/CHRG-109shrg27443.pdf [https://perma.cc/5B68-6KFX].

[166] Id. at 43.

[167] Letter from Alberto R. Gonzales, Att'y Gen., to Patrick Leahy & Arlen Specter, U.S. Sens. (Jan. 17, 2007), http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf [https://perma.cc/EG9N-L62Q].

communications worked.[168] Still, he "deplored the way the White House went about fixing the problem."[169] He disapproved of Vice President Cheney's approach of "blow[ing] through" laws like FISA "in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations."[170] In his view, the White House should have worked "with the FISA court or Congress."[171] In short, a plea for democratic authorization.

E. Ending "Total Information Awareness"

Stellar Wind didn't actually go away, but before Congress and the country really knew that, Admiral John Poindexter's anti-terrorism idea of "Total Information Awareness" ("TIA") burst into public view.[172] Poindexter, a former submarine hunter, believed that just like subs had "signatures" to allow their identification underwater, so too did terrorist organizations planning an attack.[173] His idea was that if we could just identify those signatures in an ocean of data, we could thwart terrorist attacks.[174]

Even assuming Poindexter's idea could work, it required indiscriminately collecting vast amounts of personal data.[175] An initiative of the Defense Advanced Research Projects Agency ("DARPA"), TIA sought to use "data-mining techniques" and "advanced collaborative and decision support tools" to collect Americans' sensitive personal data like phone call records, emails, financial statements, and medical

[168] Jack Goldsmith, The Terror Presidency: Law and Judgment Inside the Bush Administration 181 (2010).

[169] Id.; see also Jack Goldsmith & Tim Wu, Who Controls the Internet? 81–84 (2006) (describing techniques governments may use to attempt to control the internet).

[170] Goldsmith, supra note 168, at 181.

[171] Id. at 182.

[172] Gina Marie Stevens, Cong. Rsch. Serv., RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws (2003) (found on the third page of the unpaginated report).

[173] Friedman, supra note 151, at 292.

[174] Id.

[175] That was a big, and unwarranted, assumption. As engineer and chief IBM scientist Jeff Jonas and policy expert Jim Harper underscored, data mining is not well suited to find terrorist and identify terrorist activity, amounting to a waste of time and violating civil liberties. Jeff Jonas & Jim Harper, Effective Counterterrorism and the Limited Role of Predictive Data Mining, Cato Inst. (Dec. 11, 2006), https://www.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf [https://perma.cc/UY4V-39WZ].

documents.[176] The amassing of such information was intended "for intelligence and law enforcement use" to identify terrorists prior to an attack.[177]

There was nothing subtle about the TIA program. Its logo was the all-seeing eye from the back of a dollar bill, staring down at the entire planet, and its motto (in Latin) was "knowledge is power."[178] Conservative columnist William Safire described the breadth of data on ordinary Americans that was to be amassed by the Defense Department: "Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend . . . ."[179]

The reaction around the country could be described as ballistic, focused on the sorts of concerns about privacy, security, and executive power that were raised in the 1960s and 1970s. Members of groups as disparate as the American Civil Liberties Union, People for the American Way, Paul Weyrich's Free Congress Foundation, and the Libertarian Party joined together to write angry letters to Congress.[180] They highlighted the lack of transparency ("DARPA itself has resisted lawful requests for information"), the lack of oversight, and the fear that "[d]ata files that become available . . . are likely to be used beyond their initial purpose."[181]

[176] Gene Healy, Beware of Total Information Awareness, Cato Inst. (Jan. 20, 2003), https://www.cato.org/commentary/beware-total-information-awareness [https://perma.cc/2GBH-4FBR]; Def. Advanced Rsch. Projects Agency, U.S. Dep't of Def., Report to Congress Regarding the Terrorism Information Awareness Program: Executive Summary 1 (May 20, 2003), https://w2.eff.org/Privacy/TIA/TIA-report.pdf [https://perma.cc/2VB3-B2E7].

[177] Dep't of Def. Off. of Inspector Gen., Terrorism Information Awareness Program 5 (Dec. 12, 2003), https://www.dodig.mil/Reports/Compendium-of-Open-Recommendations/Article/1116783/terrorism-information-awareness-program/ [https://perma.cc/8P8B-P75R].

[178] Jeffrey Rosen, This Year in Ideas; Total Information Awareness, N.Y. Times (Dec. 15, 2002), https://www.nytimes.com/2002/12/15/magazine/the-year-in-ideas-total-information-awareness.html [https://perma.cc/NZW3-35ZS].

[179] William Safire, You Are a Suspect, N.Y. Times (Nov. 14, 2002), https://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html [https://perma.cc/CG2H-3CPS].

[180] Letter from Marc Rotenberg, Exec. Dir., Elec. Priv. Info. Ctr., et al., to Thomas Daschle & Trent Lott, U.S. Sens. (Nov. 18, 2002) (on file with the Electronic Privacy Information Center); Press Release, U.S. Pub. Pol'y Comm. of the Ass'n for Computing Mach., Computer Scientists Question TIA Surveillance Plan (Jan. 23, 2003) (on file with authors); Letter from ACLU et al. to Duncan Hunter & Ike Skelton, U.S. Reps., Comm. on Armed Servs. (Jan. 14, 2003) (on file with authors).

[181] Letter from Marc Rotenberg, supra note 180; Faye Bowers & Peter Grier, Why the Pentagon Will Watch Where You Shop, Christian Sci. Monitor (Dec. 3, 2002), https://www.csmonitor.com/2002/1203/p01s01-usgn.html [https://perma.cc/PS6D-BRLH].

The now-familiar harms—the erosion of privacy, the risk of discrimination, the chilling of expression, and the amassing of excess government power—were raised repeatedly.

On September 30, 2003, Congress killed TIA.[182] TIA's two biggest critics, Senators Ron Wyden and Byron Dorgan, called the program "the biggest spying and surveillance overreach in America's history," which had completely "gutt[ed] civil liberties" of all Americans.[183] After the Senate's 95-0 vote to end TIA, Senator Wyden declared: "The lights are out . . . . We're not going to have Americans who are law-abiding spied on on American soil."[184]

Still, intelligence officials and members of the executive branch do not lightly take no for an answer. Apparently, Congress must make the same point over and over again. That was about to become abundantly clear.

F. The Section 215 Program: Rejecting Indiscriminate Collection of Telephone Metadata and Setting the Terms for Its Use

About seven years after the country believed Congress had put an end to Stellar Wind, it was established—thanks to the revelations of Edward Snowden—that was not the case. Rather, the Bush Administration had gone to the FISC to get approval of both Stellar Wind programs. Federal lawmakers' ultimate resolution of those programs provided a clear understanding as to what they and the country believed was appropriate regarding indiscriminate data collection of United States persons and how

[182] William New, Congress Funds Defense, Kills Terrorism Information Awareness, Gov't Exec. (Sept. 25, 2003), https://www.govexec.com/defense/2003/09/congress-funds-defense-kills-terrorism-information-awareness/15051/ [https://perma.cc/2EYV-7YJ6]; Department of Defense Appropriations Act, Pub. L. No. 108-87, § 8131(a), 117 Stat. 1054, 1102 (2003). It is not clear that TIA was fully eliminated. A classified annex to the Appropriations Act allowed some programs to continue in other agencies so long as they were used for intelligence gathering and not against U.S. citizens. See Mark Williams Pontin, The Total Information Awareness Project Lives On, MIT Tech. Rev. (Apr. 26, 2006), https://www.technologyreview.com/2006/04/26/229286/the-total-information-awareness-project-lives-on/ [https://perma.cc/3SPG-8FGM]. A lack of transparency impedes clear understanding of what is occurring, which—as we argue *infra*—should not be the case regarding surveillance that implicates the rights of U.S. persons.

[183] Press Release, Ron Wyden, U.S. Sen., Wyden, Dorgan Continue Call for Closure of "Terrorism Information Awareness" Program (July 31, 2003), https://www.wyden.senate.gov/news/press-releases/wyden-dorgan-continue-call-for-closure-of-terrorism-information-awareness-program [https://perma.cc/E8KY-8LC5].

[184] New, supra note 182.

the collection and use of data should be regulated. This was a defining moment, setting the terms for indiscriminate data surveillance.

1. Bulk Collection Revealed and Ended

On June 6, 2013, the British newspaper *The Guardian* reported that Verizon was turning over the telephone call records of millions of Americans—eventually it became clear it was virtually every American—to the National Security Agency.[185] It emerged that for years, the FISC had been issuing secret orders requiring phone companies to turn over to the NSA all of their "call detail records" (also known as "telephone metadata") on an ongoing basis. This included what phone numbers contacted other phone numbers, when those calls were made, and how long the calls lasted.[186] The idea was that once the NSA obtained the bulk telephone metadata, officials could "query" the huge database using a phone number thought to be associated with possible terrorist activity, known as a "selector." In that way, they could find out with whom that caller was in contact, thereby identifying members of a terrorist organization.[187]

This bulk collection of telephone metadata was referred to as the "215 Program," in reference to a provision of the USA PATRIOT Act that was invoked by the government and the FISC as supposedly providing a statutory basis for it.[188] For years, relying on Section 215, the FISC had been secretly signing orders allowing this mass collection of telephone metadata and the querying of the data.[189] By its terms, Section 215

[185] Glenn Greenwald, NSA Collecting Phone Records of Millions of Verizon Customers Daily, The Guardian (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/WL3W-TBCX]; see also ACLU v. Clapper, 785 F.3d 787, 795 (2d Cir. 2015) (describing how the article from *The Guardian* brought the telephone metadata program to the attention of the American public).

[186] Sharon Bradford Franklin, Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records, Just Sec. (Mar. 28, 2019), https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/ [https://perma.cc/2X84-6ZQJ].

[187] See NSA C.L. & Priv. Off., Transparency Report: The USA FREEDOM Act Business Records FISA Implementation 5–7 (Jan. 15, 2016), https://media.defense.gov/2021/aug/18/2002833868/-1/1/0/ufa_civil_liberties_and_privacy_report.pdf [https://perma.cc/BXK4-TKYU] (providing a brief explanation of how Section 215 data was being used for searches).

[188] See *Clapper*, 785 F.3d at 793–98 (providing background on Section 215).

[189] See Priv. & C.L. 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 9 (Jan. 23, 2014) [hereinafter PCLOB Report], https://documents.pclob.gov/prod/Documents/OversightReport/cf0ce183-7935-4b06-bb41-007d1f437412

authorized the FBI to collect "tangible things," including "business records," upon a showing of "reasonable grounds to believe" that the materials collected "are relevant to an authorized investigation" directed against terrorism.[190] The government argued—and the FISC accepted—that the phone records of every single American were "relevant" to an "authorized investigation"—apparently, the generalized hunt for terrorist activity.[191] In other words, even though no person whose data was collected was suspected of anything, and in fact there was not even a specific terrorism investigation underway, the government took the position—accepted by the FISC—that all of everyone's data could be collected under Section 215 nonetheless. As the government explained to the FISC:

> [A]lthough investigators do not know *exactly* where the terrorists' communications are hiding in the billions of telephone calls flowing through the United States today, we do know they *are there*, and if we archive the data now, we will be able to use it in a targeted way to find the terrorists tomorrow.[192]

Countless news stories between the time of disclosure and the congressional vote ending the 215 Program captured Americans' disfavor of it.[193] Polls repeatedly showed the same.[194] President Barack Obama,

/215-Report_on_the_Telephone_Records_Program%20-%20Completed%20508%20-%2011292022.pdf [https://perma.cc/5D4G-MRWD].

[190] See USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88; see also *Clapper*, 785 F.3d at 793–98 (describing the statutory scheme of Section 215).

[191] See PCLOB Report, supra note 189, at 42–45.

[192] Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism at 8, [Redacted], No. BR 06-05 (FISA Ct. May 23, 2006); see also Lauren Bateman, The November NSA Trove V: Congressional Stuff, Lawfare (Nov. 21, 2013), https://www.lawfaremedia.org/article/november-nsa-trove-v-congressional-stuff [https://perma.cc/M6KJ-JSKR] (providing context for government briefing).

[193] See, e.g., Sari Horwitz & William Branigin, Lawmakers of Both Parties Voice Doubts About NSA Surveillance Programs, Wash. Post (July 17, 2013), https://www.washingtonpost.com/world/national-security/house-committee-holds-hearing-on-nsa-surveillance-programs/2013/07/17/ffc3056c-eee3-11e2-9008-61e94a7ea20d_story.html [https://perma.cc/3CC3-B8WR]; Ewen Macaskill & Gabriel Dance, NSA Files: Decoded, The Guardian (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2 [https://perma.cc/C5N3-RURA] (documenting negative reactions from elected U.S. officials, technology companies facing backlash from users, and others).

[194] See, e.g., Susan Page, Poll: Most Americans Now Oppose the NSA Program, USA Today (Jan. 20, 2014, 3:10 PM), https://www.usatoday.com/story/news/politics/2014/01/20/p

forced to deal with the Program publicly, appointed a President's Review Group ("PRG"), which issued a public report in December of 2013. Eventually, he came out against the indiscriminate collection by government of all this data and for strict constraints regarding its use.[195] The Privacy and Civil Liberties Oversight Board ("PCLOB")—the ostensible federal watchdog for matters such as these—conducted its own review, reporting in mid-January of 2014. It came to the same conclusion.[196]

It took Congress a year of contentious debate to finally resolve the matter, but when it did, its resolution—the USA FREEDOM Act of 2015—was unequivocal. Congress ended the 215 Program, clearly denouncing the sort of indiscriminate bulk collection that is the subject of this Article. Congress put in its place an alternative: (a) phone records remained in the companies' hands, not the government's possession; until (b) the government could show there was a predicate for collection of data regarding a particular selector, i.e., "reasonable, articulable suspicion" that the selector was involved in terrorism or related international activities; and even yet, (c) a court had to sign off on the existence of reasonable suspicion as to that selector.[197] The vote in Congress on the

oll-nsa-surveillance/4638551 [https://perma.cc/Z7PT-5XAM]; George Gao, What Americans Think About NSA Surveillance, National Security and Privacy, Pew Rsch. Ctr. (May 29, 2015), https://www.pewresearch.org/short-reads/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy [https://perma.cc/YA39-6BKQ] (showing that a majority of Americans oppose government bulk data collection on citizens and two-thirds believe there are not "adequate limits on what types of data can be collected").

[195] See White House Off. of the Press Sec'y, Fact Sheet: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program (Mar. 27, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m [https://perma.cc/RW8V-HRG4].

[196] See PCLOB Report, supra note 189, at 16–17 (recommending the end of the Section 215 program and the immediate implementation of additional privacy safeguards).

[197] See USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268; see also Fact Sheet: Implementation of the USA Freedom Act of 2015, Off. of the Dir. of Nat'l Intel. (Nov. 27, 2015), https://www.dni.gov/files/icotr/USAFA%20Implementation%20Fact%20Sheet.pdf [https://perma.cc/FTC6-8BRQ] (describing the rollout of the new program). The USA FREEDOM Act adopted many of the changes suggested by the President's Review Group. See Peter Swire, The USA FREEDOM ACT, the President's Review Group, and the Biggest Intelligence Reform in 40 Years, IAPP (June 8, 2015), https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years/ [https://perma.cc/624C-GGHN].

USA FREEDOM Act was lopsided: in the House of Representatives, it was 338-88; in the Senate, 67-32.[198]

2. Legal Limits

What's notable about the adoption of the USA FREEDOM Act of 2015 is how much agreement there was on critical points, even from those who favored maintaining some vestige of the 215 Program. It is here that we get our clearest window into the rejection of indiscriminate bulk collection of U.S. persons' data—even for such a dire concern as terrorism—and also what relevant actors in and out of Congress believed was required before any data was collected or used. In short, the debate over the 215 Program provides a roadmap for distinguishing acceptable from unacceptable law enforcement data surveillance practices.

a. Legislative Authorization Is Essential

Once the Bush Administration's Stellar Wind surveillance program became public, *no one* expressed the view that this sort of indiscriminate bulk collection would be appropriate without *legislative authorization*. Although the FISC bought the Administration's argument that *everyone's* phone records were relevant to an ongoing, generalized investigation into terrorism, almost everyone else rejected it.[199] Republican Representative James Sensenbrenner of Illinois, the author of the USA PATRIOT Act that had adopted Section 215 originally and the leader of compromise that led to the enactment of the USA FREEDOM Act, said in debate, "We are here today . . . because the government has misapplied the law that we passed."[200] Democratic Representative Jerrold Nadler, the Ranking

[198] USA Freedom Act, House of Reps. Judiciary Comm., https://judiciary.house.gov/usa-freedom-act#:~:text=Bill%20Status%3A%20On%20May%2013,Act%20on%20June%202%2C%202015 [https://perma.cc/5PRT-25MC] (last visited May 16, 2024).

[199] See, e.g., PCLOB Report, supra note 189, at 10 ("There are four grounds upon which we find that the telephone records program fails to comply with Section 215."); President's Rev. Grp. on Intel. & Commc'ns Techs., Liberty and Security in a Changing World 86–88 (2013) [hereinafter President's Review Group Report] (discussing its disagreement with the FISC's interpretation of Section 215); 161 Cong. Rec. H2916 (daily ed. May 13, 2015) (statement of Rep. James Sensenbrenner) ("[A] clean reauthorization would be irresponsible. Congress never intended section 215 to allow bulk collection. That program is illegal and based on a blatant misinterpretation of the law.").

[200] USA Freedom Act: Markup of H.R. 3361 Before the H. Comm. on the Judiciary, 113th Cong. 11 (2014) [hereinafter House Markup 2014] (statement of Rep. James Sensenbrenner). This was a markup of a bill that ultimately was not adopted and which, once it came to the floor, did not even reflect that markup. As Rep. Zoe Lofgren and then-Rep. Jared Polis noted,

Member of the House Judiciary Committee, said "Congress never intended to authorize this type of unchecked, sweeping surveillance of our citizens."[201] The most that defenders of the 215 Program could bring themselves to say was that the legal question of authorization was a "difficult one" and it was a "reasonable reading" of the statute, "made in good faith by numerous officials in two Administrations of different parties."[202]

b. Searching Without Reasonable Suspicion Is Unacceptable

The next point of agreement was that before government officials could access the data of any individual, they needed a constitutionally sufficient predicate to do so. Understand that in all bulk collection programs, there are two distinct steps. First, data is *collected*. Second, it is "*queried*" to obtain information as to specific individuals.

Although there was disagreement about whether the government should be able to collect and hold the data itself, or whether it must remain with the companies, *no one* argued individual data could be queried in the absence of a showing of "reasonable articulable suspicion" ("RAS")—in this case, that the selection term related to a foreign power. Defending the 215 Program before Congress, Deputy Attorney General James Cole explained that, even under the existing program, in which the data remained with the government, "[y]ou can't just wander through all of these records. There are very strict limitations . . . . You have to have reasonable, articulable suspicion that a specific phone number, which they call a selector, is involved with one of these specified terrorist organizations."[203]

When Congress acted to end the 215 Program and require the data be held by the private companies, not the government, it wrote the RAS

the marked-up bill was "secretly" changed overnight before it came to the floor. 160 Cong. Rec. H4710 (daily ed. May 21, 2014) (statement of Rep. Zoe Lofgren) ("I think it is ironic that a bill that was intended to increase transparency was secretly changed between the committee markup and its floor consideration . . . in worrisome ways."). However, the bill that ultimately was adopted reflected the 2014 markup. See ACLU v. Clapper, 785 F.3d 787, 799 (2d Cir. 2015) (discussing modifications to the Freedom Act from the initial versions introduced in 2014, compared to the version passed in 2015).

[201] House Markup 2014, supra note 200, at 15.

[202] PCLOB Report, supra note 189, at 210, 215 (providing a separate statement by board member Rachel Brand, which includes her partial dissent from the report's analysis).

[203] The Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary, 113th Cong. 14–15 (2013) [hereinafter FISA Authorities Hearing 2013].

standard into law as the basis for government accessing the data from the companies who held it. As Representative James Sensenbrenner put it, "For counterterrorism purposes only, the government can use a specific selection term to get detailed records when it has reasonable articulable suspicion that the selection term is associated with a foreign power or an agent of a foreign power."[204]

c. Reasonable Suspicion Must Be Approved by a Court

Congress also made clear that (absent an emergency) the existence of the predicate of reasonable suspicion had to be recognized by a court, much like courts issue warrants in domestic cases. As Deputy Attorney General Cole's comment indicated, the FISC had allowed high government officials to make this determination themselves. And, to be clear, there had been very few queries annually—as few as three hundred.[205] Nonetheless, Congress said no to self-regulation: the existence of RAS was for a court to decide. Republican Representative Bob Goodlatte, chairing the House Judiciary Committee during markup, stressed the difference between prior practice and what Congress ultimately concluded: "Under this amendment, the FISA court, rather than the government, will be required to make a finding that a reasonable, articulable suspicion exists . . . ."[206]

d. Condemning Bulk Collection and Retention by the Government

Most important, Congress concluded that bulk collection and retention by the government of the data of innocent Americans simply was unacceptable, and had to be stopped. As Representative Nadler explained, "The companies, not the government, keep the underlying records, which can only be searched using specific selection terms designed to return only those records that are relevant to a real terrorism investigation."[207] "Above all else," as Representative John Conyers of Michigan put it—echoed by many people on both sides of the aisle—"the USA FREEDOM

[204] House Markup 2014, supra note 200, at 12.

[205] FISA Authorities Hearing 2013, supra note 203, at 10 (statement of John C. Inglis, Deputy Dir., Nat'l Sec. Agency).

[206] House Markup 2014, supra note 200, at 18. The House Report similarly explained that "the new framework requires the FISC to approve each selector for use in queries." H.R. Rep. No. 113-452, pt. 1, at 14 (2014).

[207] House Markup 2014, supra note 200, at 16.

Act represents the consensus view that all domestic bulk collection must end."[208]

This was not an easy or hasty decision: those involved in the debate understood that the decision rested on a balance between the harms of terrorism and the harms of allowing the government to collect this sort of data. What was determinative for those who favored allowing indiscriminate bulk collection, and a matter to keep in mind given today's widespread domestic data gathering, was its efficacy in preventing grave harm. As Senator Burr explained during floor debate, "We are down here battling on the Floor, those of us either on the [Intelligence Committee] or who have been on the committee since 9/11, because we have seen the impact of this program."[209] (Many, however, doubted that efficacy, which may well explain the difference in treatment by Congress of the Section 215 Program and the 702 Program, which we take up next.[210])

By wide margins, Congress deemed the risks to individual liberty and of government tyranny great enough to end bulk collection entirely. As Representative Goodlatte, who had shepherded the measure through the House Judiciary Committee and later the House itself, explained in opening debate, the bill under consideration "affirmatively ends the indiscriminate bulk collection of telephone metadata. But it goes much further than this. It prohibits the bulk collection of all records under" various authorities.[211]

3. The Dubious Constitutionality of Bulk Collection

Finally, some members of Congress were explicit that indiscriminate bulk collection of Americans' data was both unacceptable and

[208] Id. at 7.

[209] 161 Cong. Rec. S3375 (daily ed. June 1, 2015); see also FISA Authorities Hearing 2013, supra note 203, at 3 (statement of Rep. John Conyers) (discussing the "proper balance between our safety and our constitutional right to privacy"); 160 Cong. Rec. H4705 (daily ed. May 21, 2014) (statement of Rep. J. Randy Forbes) (discussing the "balance between safeguarding privacy and protecting Americans").

[210] See infra notes 267–70 and accompanying text; see also PCLOB Report, supra note 189, at 146 ("[W]e see little evidence that the unique capabilities provided by NSA's *bulk* collection of telephone records actually have yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program.").

[211] 161 Cong. Rec. H2914 (daily ed. May 13, 2015). Other representatives made statements to a similar effect. See 161 Cong. Rec. H2915 (daily ed. May 13, 2015) (statement of Rep. Bob Conyers) ("This legislation ends bulk collection . . . ."); 161 Cong. Rec. H2916 (daily ed. May 13, 2015) (statement of Rep. Jim Sensenbrenner) ("The USA FREEDOM Act also ends bulk collections across all domestic surveillance authorities, not just section 215.").

unconstitutional.[212] At the time, Supreme Court precedent could be—and was—cited to support bulk collection, underscoring just how lopsided the vote against bulk collection was. (We cannot know, of course, how many who voted against bulk collection did so on constitutional grounds.)

For those who defended the constitutionality of bulk collection, including the FISC itself, the key was the Supreme Court decision in *Smith v. Maryland*.[213] The Supreme Court held in *Smith* that because telephone users "voluntarily" give their phone information to the telephone company, the government needed neither any level of suspicion nor judicial process such as a warrant to obtain the information.[214]

For others, though, it did not take a lot of consideration to recognize the stark difference between the NSA's collection and *Smith*. *Smith*, whether one believed it right or wrong, involved the search of the telephone metadata of a single individual for whom there clearly was suspicion of serious wrongdoing. The NSA, on the other hand, collected the telephone metadata of every single U.S. person, the overwhelming majority of whom were suspected of nothing.

As Representative Sensenbrenner put it, the FISC had "opened the floodgate to a practice of bulk collection that was never before possible, let alone legal, in our country's history."[215] Representative Nadler, a longtime member of the House Judiciary Committee, lost all patience with one Obama Administration witness defending the collection: "Oh, come on," he responded, exasperated, "[a]re there any—are there any instances in the history of the United States that you know of where a grand jury subpoena said get every—get all information other than the content of a telephone call of all telephone calls in the United States, or anything like that?"[216] Senator Rand Paul pointed out: "We are not collecting the information of spies. We are not collecting the information of terrorists. We are collecting all American citizens' records all of the

[212] See, e.g., 161 Cong. Rec. H2920 (daily ed. May 13, 2015) (statement of Rep. Hakeem Jeffries) ("This overreach was unnecessary, unacceptable, and unconstitutional.").

[213] 442 U.S. 735, 745–46 (1979).

[214] Id. at 745. The FISC stood by this conclusion even as the Supreme Court started to recognize the problem with digital data collection in *United States v. Jones*, 565 U.S. 400, 417 (2012). It simply said: "Smith remains controlling." In re Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, 2014 WL 5463097, at *11 (FISA Ct. Mar. 20, 2014) (Collyer, J.); In re Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 13-158, slip op. at 5 (FISA Ct. Oct. 11, 2013) (McLaughlin, J.).

[215] House Markup 2014, supra note 200, at 11.

[216] FISA Authorities Hearing 2013, supra note 203, at 23.

time. This is what we fought the Revolution over."[217] His point was echoed by Representative Nadler, who called the metadata collection "the contemporary equivalent of the British writs of assistance that early American revolutionaries opposed and that the Fourth Amendment was drafted to outlaw."[218] Representative Conyers maintained that "metadata collected in such a super-aggregated fashion can amount to a Fourth Amendment violation."[219]

G. Section 702: An Exception That Proves the Rule

Which brings us, finally, to the continuing controversy around the other half of what had been Stellar Wind, the targeting of foreign persons and entities abroad under Section 702 of FISA. It's controversial not because foreigners abroad are targeted, so much as because in doing so, Section 702 collects communications of Americans as well as foreigners, and those communications are queried by the FBI under certain circumstances.[220] To this day, this aspect of the 702 program has remained the subject of fierce debate—as it should be.

The ongoing battle over Section 702—which is on the very edge of acceptability in the eyes of some, and tilting over it in the eyes of others—is revealing as to congressional thinking regarding the boundaries of indiscriminate data surveillance. Its foreign intelligence imperatives push constantly for renewal, while its domestic implications have made it a battleground. As this Article was headed to print, Section 702 was renewed for just two years (rather than the typical five), with important changes made (some helpful and some problematic) and promises of more to come.[221]

---

[217] 161 Cong. Rec. 7865 (daily ed. May 31, 2015).

[218] 161 Cong. Rec. 6616 (daily ed. May 13, 2015).

[219] FISA Authorities Hearing 2013, supra note 203, at 16.

[220] See Priv. & C.L. Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 55–59 (July 2, 2014) [hereinafter PCLOB 2014 702 Report], https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf [https://perma.cc/8W72-6ZEM] (detailing the incidental collection of American communications during routine 702 surveillance).

[221] Section 702 was reauthorized for four months at the end of 2023. National Defense Authorization Act for Fiscal Year 2024, H.R. 2670, 118th Cong. (2023) (signed by the President on Dec. 22, 2023); National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136, 1108 (2023) (codified in scattered sections of the U.S. Code). Then, on the brink of that expiration, it was reauthorized. See NPR, supra note 21. However, that reauthorization was for two years, not the usual five. Marquis & Reynolds, supra note 21;

Wherever the struggle over Section 702 ultimately ends up—should it come to a resting place—several things distinguish it from the purely domestic indiscriminate data surveillance that is the subject of this Article. Section 702's exceptional treatment of non-U.S. persons' internet and telecommunications data provides further insights. First, there is wide consensus in Congress that the program is efficacious. Second, that efficaciousness is in the realm of national security, and all agree that the national security realm is special; that what plays there will not and should not be permitted with regard to domestic policing. Third, Americans' data is not being collected indiscriminately, though it is being collected as a consequence of collection from non-U.S. persons. Fourth, even then, Section 702 has a litany of safeguards and oversight that stands in stark contrast to the collection and querying of personal information under the domestic programs described in Part I. Finally, for the most part, the changes that have been made along the way with Section 702, while in the main inadequate, and the continuing fight over the inadequacy of those changes, point in general toward recognition that there is and must be closer control over domestic surveillance.

1. What 702 Does

Proponents of Section 702 collection claim that unlike the indiscriminate collection under Section 215, it is targeted—against specific foreigners abroad—but this is a bit of a misnomer, because under Section 702, the government collects and retains vast amounts of Americans' data.[222] Under Section 702, the FISC approves certifications from the government that contain targeting rules pursuant to which the NSA compels providers to give them internet and telephone communications of foreign persons abroad who are reasonably believed

see also Aaron, supra note 22. The reforms are described infra notes 252–57 and accompanying text.

[222] See, e.g., 115 Cong. Rec. H142 (daily ed. Jan. 11, 2018) (statement of Rep. Christopher Stewart) ("Section 702 is a targeted program, with roughly 106,000 foreign targets worldwide . . . [out of a worldwide population of] about 7.5 billion . . . [so] this program can hardly be described as bulk collection."); see PCLOB 2014 702 Report, supra note 220, at 103 ("Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons . . . . The program does not operate by collecting communications in bulk.").

to be a source of foreign intelligence information or a threat to the national security.[223]

The problem with this claim about targeting is that once a foreign target is identified, *all* of the content related to their communications—including that with Americans—is collected, stored, and at times queried. As of 2011, the NSA was storing some 250 million communications annually, and everyone involved in the debate over Section 702 assumes that number has risen dramatically since then, especially because the number of foreign targets itself has increased significantly in the intervening years.[224] This is not just metadata being collected, like with the shuttered 215 Program. The Section 702 Program gathers "content" of internet and telephone communications that can be "highly personal and sensitive," and sweeps in many Americans "innocent of any complicity in terrorist or other activity of foreign intelligence interest."[225]

As applied to U.S. persons, the constitutionality of Section 702 is deeply contested. That is because once the data is collected, the FBI queries the collected data, including the content of Americans' communications, without any predicate whatsoever. One defense of the collection and retention of Americans' private communications is that it is simply "incidental" to the targeted collection from foreigners abroad—but this is a misnomer.[226] In truth, the government very much wants (and gets) access to the information. As Attorney General Michael Mukasey explained in a letter to Senate Majority Leader Harry Reid, digital

[223] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2440–41, 2446–47 (codified as amended at 50 U.S.C. § 1881a); 15 U.S.C. § 1805.

[224] See Off. of C.L., Priv. & Transparency, Off. of the Dir. of Nat'l Intel., Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2021, at 17 (2022); Ctr. for Democracy & Tech., Comment to the Privacy and Civil Liberties Oversight Board Regarding Examination of and Reforms to Section 702 of the Foreign Intelligence Surveillance Act 2 (2022) (citing a 118% increase in the number of known targets between 2018 and 2022 based on yearly DNI reports).

[225] PCLOB 2014 702 Report, supra note 220, at 112, 153; accord Priv. & C.L. Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 11 (Sep. 28, 2023) [hereinafter PCLOB 2023 702 Report], https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf [https://perma.cc/4YZE-BXKP]. But see id. at B-15 to -16 (arguing that the Section 702 database contains a small amount of U.S. persons information and content is rarely retrieved).

[226] See Jeramie D. Scott, Reforming 702: End Warrantless Backdoor Searches, Elec. Priv. Info. Ctr. (Feb. 23, 2023), https://epic.org/reforming-702-end-warrantless-backdoor-searches/ [https://perma.cc/GWP8-FJ7X].

communications with foreign targets are "precisely the communication[s] we generally care most about."[227] That's why these are referred to colloquially and commonly as "backdoor searches."[228]

Those who believe that Section 702 is constitutional (including the FISC) argue that the collection of communications of foreigners abroad is fine under existing Supreme Court precedents, and the initial collection being lawful, *anything* incidentally caught up in the course of collection can be stored and examined at will.[229] The U.S. Court of Appeals for the Second Circuit has held, contrary to the FISC, that although collecting and holding the data might be constitutional, querying it without a warrant was not.[230] As Representative Jim Jordan said, putting it in plain language, "'[Q]uery' is a fancy way of saying 'search,'" and under Section 702, the government searches many innocent Americans' actual communications without a warrant, or indeed any judicial process at

[227] Letter from Michael B. Mukasey, Att'y Gen., to Harry Reid, Senate Majority Leader, 4 (Feb. 5, 2008).

[228] See Scott, supra note 226 ("A warrantless backdoor search is a search of Americans' communications 'incidentally' collected under Section 702.").

[229] See, e.g., Redacted FISC Memorandum Opinion and Order, slip op. at 36–45 (FISA Ct. Nov. 6, 2015), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/20151106-702Mem_Opinion_Order_for_Public_Release.pdf [https://perma.cc/84KA-RXV3]) (concluding that Section 702's targeting and minimization procedures are consistent with the Fourth Amendment). This argument rests on Supreme Court precedents quite unlike what Section 702 involves. The first step is supported by the nonapplicability of Fourth Amendment protections to searches conducted abroad, which was approved in a case involving the arrest abroad of a foreign citizen. See United States v. Verdugo-Urquidez, 494 U.S. 259, 261–62 (1990). The second is supported by cases under long-established doctrines involving the searches of an individual person's data, holding once law enforcement gains information incidental to a lawful search, it can use that information. See United States v. Muhtorov, 20 F.4th 558, 598 (10th Cir. 2021) (holding incidental collection lawful on the basis of incidental overhear doctrine and plain view doctrine); see also id. at 595 ("[I]f there had been a warrant to search a home . . . 'a subsequent seizure of . . . records' bearing the handwriting of someone not identified in the warrant would comport with the Fourth Amendment." (discussing United States v. Kahn, 415 U.S. 143, 155 n.15 (1974))); accord 115 Cong. Rec. H142 (daily ed. Jan. 11, 2018) (statement of Rep. Christopher Stewart) ("The Fourth Amendment, as interpreted by numerous Federal courts, does not require the FBI to obtain a separate order from the FISC to review lawfully acquired 702 information."). The latest Section 702 Report from the PCLOB contains yet another debate over the constitutionality of querying U.S. persons data. Compare PCLOB 2023 702 Report, supra note 225, at A-2 to -3 (separate statement of Chair Sharon Bradford Franklin) (arguing querying without sufficient cause violates the Constitution), with id. at B-8 to -9 (separate statement of Board Members Beth A. Williams and Richard E. DiZinno) (arguing querying does not violate the Constitution).

[230] United States v. Hasbajrami, 945 F.3d 641, 670 (2d Cir. 2019).

all.[231] Representative Ted Lieu similarly put it, "[S]pying on foreigners without following the Constitution, that is okay; spying on Americans without following the Constitution, that is not okay. The Fourth Amendment does not have an asterisk that says our intelligence agencies don't have to follow it."[232]

Prior to the very recent reauthorization, Section 702 was last amended in 2018, and while proponents said changes made at that time improved the situation regarding Section 702's constitutionality, critics disagreed. The theory of the 2018 amendments was that to query the part of the 702 database held by the FBI for a purely criminal (i.e., not national security) case, the FBI had to get a warrant from the FISC. If no warrant was obtained, the government could not "use" the communications in a criminal trial. The first and biggest problem with this is that the warrant requirement only applied to "predicated" investigations, i.e., if the FBI already had cause to believe a non-national security criminal offense was occurring. Yet the FBI was (and is) querying the database at an earlier "assessment" stage of inquiry, before it has cause, hundreds of thousands of times annually without any judicial process. Even then, in the rare case in which a warrant might be needed, there are statutory exceptions to both the query and use rules that are wide enough to drive a truck through: for example, the Attorney General could deem the "use" lawful in many circumstances, and that decision itself was immune from judicial review.[233] In addition, although the warrant requirement nonetheless has been triggered approximately 100 times since the 2018 amendments, the FBI never once has obtained one.[234]

[231] See The U.S.A. Liberty Act of 2017: Markup of H.R. 3989 Before the H. Comm. on the Judiciary, 115th Cong. 82 (2017) [hereinafter USA Liberty Act Markup] (statement of Rep. Jim Jordan).

[232] 115 Cong. Rec. H155 (daily ed. Jan. 11, 2018) (statement of Rep. Ted Lieu).

[233] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 102, 132 Stat. 3, 8 (2018) (permitting the use of information acquired under Section 702 if the Attorney General determines that the criminal proceeding involves certain crimes or "affects, involves, or is related to the national security of the United States").

[234] Fixing FISA, Part II: Hearing Before the Subcomm. on Crime & Fed. Gov't Surveillance of the H. Comm. on the Judiciary, 118th Cong. 14 (2023) (testimony of Elizabeth Goitein, Senior Director, Liberty and National Security Program, Brennan Center for Justice at New York University School of Law) (citing annual statistical transparency reports by the Office of the Director of National Intelligence); see also PCLOB 2023 702 Report, supra note 225, at 187 ("Particularly troubling is that the FBI has never once submitted an application to the FISC pursuant to Section 702(f)(2), despite many documented cases over the past five years (since the requirement was enacted) in which the warrant requirement actually applied.").

2. Efficacy and Evasion

Despite reasonable questions about its constitutionality as it applies to the communications of Americans, Section 702 has survived largely because of a good faith struggle among legislators to arrive at the right balance between liberty and national security. Still, in trying to resolve this question, they are hampered by a lack of candor and assistance by officials in the Intelligence Community.

There is widespread consensus that Section 702 is a vital and valuable part of the apparatus for preserving the national security of the United States.[235] Even those in Congress who have been seriously frustrated and concerned about the failure to reform Section 702 see its value. Representative Jim Himes of Connecticut failed to get his proposed amendments to the 2018 reauthorization to the floor, yet described in moving detail how Intelligence Committee members daily "descend in the bowels of this Capitol" to "hear about some of the most grotesque threats to American safety and interests that you can imagine" and stressed "how essential 702 authorities are."[236]

What no one seems to know for sure, though, is just how essential a part is played by the collection and querying of Americans' information, and how much that would be hampered with legal restrictions that would bring it closer to constitutionality. (Although there are many indications that valid purposes would not be hampered much at all.[237]) Here, the

[235] See Chris Fonzone, George Barnes, David Cohen, Paul Abbate & Matthew Olsen, Joint Statement for the Record of the Senate Judiciary Committee 2 (June 13, 2023) [hereinafter IC Joint Statement 2023], https://www.judiciary.senate.gov/imo/media/doc/2023-06-13%20-%20Joint%20statement%20-%20ODNI,%20NSA,%20CIA,%20FBI,%20DOJ%20(1).pdf [https://perma.cc/JJ7Z-ZTXX] ("Section 702 . . . is indispensable to protect the nation against national security threats. It has proved invaluable in protecting American lives and U.S. national security."); see also PCLOB 2023 702 Report, supra note 225, at 7 (reporting that "the United States is safer with the Section 702 program than without it" and the program "has been highly valuable in protecting the United States from a wide range of foreign threats").

[236] 115 Cong. Rec. H158 (daily ed. Jan. 11, 2018) (statement of Rep. Jim Himes).

[237] Many in the civil liberties community have looked into the issue and concluded that a warrant requirement for U.S. person queries would not hamper Section 702's mission. See, e.g., Jake Laperruque, The Government's Objections to FISA 702 Reform Are Paper Thin, Lawfare (July 7, 2023, 10:00 AM), https://www.lawfaremedia.org/article/the-government-s-objections-to-fisa-702-reform-are-paper-thin [https://perma.cc/NR24-5Z3T]; Noah Chauvin, Surveillance Reforms Do Not Endanger Americans, Brennan Ctr. for Just. (July 19, 2023), https://www.brennancenter.org/our-work/analysis-opinion/surveillance-reforms-do-not-endanger-americans [https://perma.cc/BZ96-ELVR]; Patrick C. Toomey, Sarah Taitz & Kia Hamadanchy, The Government's Section 702 Playbook Doesn't Work Anymore, Just Sec. (Aug. 30, 2023), https://www.justsecurity.org/87893/the-governments-section-702-playbook-

ongoing problem has been a troubling lack of candor and cooperation on the part of the Intelligence Community in helping legislators work their way through this.

Transparency has been the issue from the start. The FBI insisted it lacked the technical ability to provide information on U.S. person queries, but then Congress put a requirement in the statute to provide more information.[238] The FBI ignored this, until the FISC made clear it had to happen. Then, all of a sudden, the technically impossible became possible.[239] It also appears the Intelligence Community regularly cherry-picks details of the use of 702 it chooses to declassify, in order to show 702's importance, rather than finding some way to describe systematically what 702 accomplishes and does not through querying of Americans' data.[240] Bipartisan frustration over the conduct of the FBI around Section 702 erupted into public view during the 2018 reauthorization debate. Representative Zoe Lofgren, a Democrat, complained: "We do not know very much about what the FBI is doing because they have refused to give us information."[241] So did Representative Louie Gohmert, a Republican: "We have the people in here and ask them to give us the information on how many times that has been done, that you just stuck in an American citizen's cell phone number to do queries, just to see what is out there. And we have not gotten that

doesnt-work-anymore/ [https://perma.cc/52HY-3HV9]. Of course, looking into the question is itself hampered by the fact that much of the information is classified. Still, the PCLOB had access to that information and concluded there was "little justification" for many FBI searches and that "[t]he FBI identified few cases in which a U.S. person query provided unique value in demonstrating a previously unknown connection between the U.S. person and another Section 702 target or otherwise advancing a criminal investigation." PCLOB 2023 702 Report, supra note 225, at 190. The greatest value is for what are called "defensive" queries, for example helping victims or targets of cyberattacks. Id. at 168. Of course, for these there may be consent for the searches, or the matter could perhaps be dealt with statutorily. For what it is worth, several former national security officials do not oppose a warrant requirement. See, e.g., President's Review Group Report, supra note 199, at 29; David Aaron, Expert Q&A with David Aaron on FISA Section 702 Reauthorization and Reform, Just Sec. (Oct. 11, 2023), https://www.justsecurity.org/89387/expert-qa-with-david-aaron-on-fisa-section-702-reauthorization-and-reform/ [https://perma.cc/F2BA-ELQG] (asserting that a warrant requirement with an emergency provision would "allow officers to obtain the information they need and move as quickly as necessary, just as they have historically done").

[238] Elizabeth Goitein, The Year of Section 702 Reform, Part I: Backdoor Searches, Just Sec. (Feb. 13, 2023), https://www.justsecurity.org/85068/the-year-of-section-702-reform-part-i-backdoor-searches/ [https://perma.cc/YV2U-PV83].

[239] Id.

[240] IC Joint Statement 2023, supra note 235, at 5.

[241] USA Liberty Act Markup, supra note 231, at 31 (statement of Rep. Zoe Lofgren).

information."[242] In its 2023 report on Section 702, the PCLOB majority condemned the lack of information on this very question but concluded that, based on what we do know, the FBI "may not need the authority to run U.S. person queries for evidence of a crime only purposes."[243]

3. Stunning Revelations and the 2024 Fight

Just as Section 702 was up for renewal, stunning revelations about the use of Section 702 to gather information on Americans keep coming out. In a decision handed down in 2022, but not declassified until a year later, the FISC stated that "compliance problems with the FBI's querying of Section 702 information have proven to be persistent and widespread."[244] It turns out the FBI ran "batch" queries—in which analysts submitted large numbers of names to be searched at once—on people arrested during Black Lives Matter protests after George Floyd was murdered by Minneapolis police. It did the same on people suspected in the January 6 insurrection. The FBI ran a batch inquiry on 19,000 donors to a congressional campaign. FISC opinions also show the FBI searched the 702 database for people it was vetting to be confidential sources, for people who came to the FBI to perform repairs, and even people who wanted to participate in the FBI's "Citizens Academy."[245] Batch inquiries consistently were performed with boilerplate justification, rather than the factual predicate the FISC has required. They are conducted with no reason to believe the query will turn up evidence of a crime or foreign intelligence information.

When at long last the FBI finally released figures on the number of U.S. person selectors it searched annually, the numbers were staggering. (Recognize, though, that there may be a number of selectors for any one

[242] Id. at 56 (statement of Rep. Louie Gohmert).

[243] PCLOB 2023 702 Report, supra note 225, at 189; see id. at 180 ("There is currently no data or transparency identifying the magnitude of incidental collection of U.S. person information."); see also id. at 188–89.

[244] Redacted FISC Memorandum Opinion and Order, slip op. at 49 (FISA Ct. Apr. 21, 2022), https://s3.documentcloud.org/documents/23817109/adb47f54-b772-4099-b0c9-adf24ef64faa.pdf [https://perma.cc/G9K8-DEH6].

[245] See Elizabeth Goitein, Protecting Americans from Warrantless Surveillance, Brennan Ctr. for Just. (Dec. 6, 2023), https://www.brennancenter.org/our-work/analysis-opinion/protecting-americans-warrantless-surveillance [https://perma.cc/D3FM-V9YJ]; Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 58 (Dec. 2021), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf [https://perma.cc/4LVQ-SQB4].

person, so the number of U.S. persons whose communications were searched may well be far lower.) From December 2020 to November 2021, there were over three million searches based on U.S. person selectors.[246] The year before, there were around 850,000—the difference was explained by the need to conduct searches to protect victims of a cybersecurity breach.[247] The latest statements from the Intelligence Community assert that after certain adjustments were made—clarifying rules, more training, and the like—the number from December 2021 to November 2022 dropped to 120,000 U.S. person searches.[248] This is indeed progress, and who's to say what the right number is without meaningful transparency and better information about efficacy. But this late in the game, it is hard to see patting oneself on the back for fixing some major violations of the rules, while it seems apparent others are ongoing.

Despite serious concerns about the way Section 702 was being used domestically, in April 2024, Congress reauthorized it.[249] As noted above, the reauthorization was only for two years, and yet it attracted a large number of "no" votes: in the House the ultimate vote for passage was 273-

[246] See Off. of C.L., Priv. & Transparency, Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities Calendar Year 2022, at 24 (2023) [hereinafter ASTR 2022]. While the FBI reported just under 3 million "de-duplicated" searches based on USP selectors, the total number of queries was nearly 3.4 million. Because an individual's rights are implicated with each search of an email address or phone number, the duplicated number is more relevant here. Id.

[247] Id.; see id. at 23 ("In the first half of 2021, a number of large batch jobs were run related to one particular investigation involving attempts by foreign cyber actors to compromise U.S. critical infrastructure. These queries . . . accounted for the vast majority of the increase in U.S. person queries . . . ."). As Elizabeth Goitein also points out, when officials defend their actions to protect victims, that is not an exception to the Fourth Amendment either. See Elizabeth Goitein, An Opportunity to Stop Warrantless Spying on Americans, Brennan Ctr. for Just. (Feb. 14, 2023), https://www.brennancenter.org/our-work/analysis-opinion/opportunity-stop-warrantless-spying-americans [https://perma.cc/ATL7-H5HP].

[248] See ASTR 2022, supra note 246, at 24.

[249] See Ryan Tarinelli, Senate Sends Surveillance Reauthorization Bill to Biden's Desk, Roll Call (Apr. 20, 2024, 8:06 AM), https://rollcall.com/2024/04/20/senate-sends-surveillance-reauthorization-bill-to-bidens-desk/ [https://perma.cc/7N8Q-KTMA].

147; and in the Senate it was 60-34.[250] Notably, these vote counts were bipartisan on both sides; this was no party-line effort.[251]

As indicated by the title of the 2024 bill—the Reforming Intelligence and Securing America Act—reauthorization involved important changes to Section 702.[252] Many of the changes were designed to limit FBI authority to search U.S. persons' communications and to address FBI misconduct, codifying changes that already had been instituted administratively.[253] The closest fight was over whether to impose a warrant requirement on such queries, and in a sign of the degree of controversy over Section 702, that measure failed in the House by a tie vote.[254] In its place, Congress imposed other restrictions, among them that a FBI supervisor or attorney must review all U.S. person queries, sharply

[250] See id.; see also Ryan Tarinelli, House Approves Surveillance Authority Reauthorization Bill, Roll Call (Apr. 12, 2024, 2:12 PM) [hereinafter Tarinelli, House Approves], https://rollcall.com/2024/04/12/house-approves-surveillance-authority-reauthorization-bill/ [https://perma.cc/9GZX-BKRC]; supra note 21 and accompanying text.

[251] Tarinelli, House Approves, supra note 250.

[252] One deeply controversial amendment expanded the definition of an "electronic communication service provider," largely to deal with the changing nature of internet communications. Marquis & Reynolds, supra note 21. Critics pointed out that the new definition could include "virtually any American business that provides its customers with Wi-Fi," a point driven home by the fact that on final passage there was an exception for "ordinary places such as senior centers, hotels, and coffee shops." Chauvin, supra note 22; Marc Zwillinger, Steve Lane & Jacob Sommer, FISA 702 Reauthorization Amendments: The Second Time Is Not the Charm, ZwillGenBlog (Apr. 9, 2024), https://www.zwillgen.com/law-enforcement/fisa-702-reauthorization-amendments-second-time-not-charm/ [https://perma.cc/22EY-NY5R].

[253] Agents must affirmatively opt in to search Section 702 material, while previously it was an opt out. Marquis & Reynolds, supra note 21; see also Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, § 2(a), 138 Stat. 862 (2024) (codified as amended at 50 U.S.C. § 1881a) (requiring FBI personnel to obtain "prior approval" from a supervisor or attorney to access certain data). Further, additional approval is needed before submitting "batch" inquiries. See id. § 2(d)(ii)(III) (requiring FBI approval for the use of "batch" technology). Referring to the administratively imposed changes, the Department of Justice said that they had "effectively eliminated instances of noncompliance with the government's querying requirements." Marquis & Reynolds, supra note 21 (citing U.S. Dep't of Just., FBI Remedial Measures Produce ~98% Query Compliance Rate, https://www.justice.gov/nsd/media/1344761/dl?inline= [https://perma.cc/ES45-MVRR] (last visited May 16, 2024)). Critics such as the Brennan Center argue the changes are "demonstrably inadequate to prevent abuses." Chauvin, supra note 22. For an argument that the long-held view of the executive branch, grounded in actual practice, is that the "national security exception" held that evidence may be collected in the interest of national security, but not used in a criminal case, see L. Rush Atkinson, The Fourth Amendment's National Security Exception: Its History and Limits, 66 Vand. L. Rev. 1343, 1347 (2013).

[254] Tarinelli, House Approves, supra note 250.

restricting the number of people who could authorize such queries and ensuring there was "a metaphorical 'grownup in the room.'"[255] Many of the legislative reforms were designed to increase transparency over the use of Section 702, such as a presumption in favor of the appointment of an amicus in FISC proceedings in cases involving the section, preparation of transcripts of FISC proceedings, time limits on publicly releasing declassified versions of FISC hearings and opinions, as well as additional reporting requirements on the extent of FBI queries, and a provision allowing congressional leaders to attend FISC hearings.[256] And, it is clear that the effort to reform Section 702 is not yet over. The bill creates a FISA Reform Commission to "consider ongoing reforms," and leadership has promised attention to these as early as the summer of 2024.[257]

4. Section 702 as a Baseline Against Which to Measure Domestic Surveillance

For all the justifiable doubt about Section 702's constitutionality, and serious concerns about the behavior of the FBI, three things about Section 702 serve as a baseline against which to measure the domestic surveillance we return to next.

The first, mentioned above, is efficacy. Although there is imperfect information still, quite unlike the situation with domestic policing, there is strong consensus based on tangible information viewed by many members of Congress that the 702 Program is critical to America's national security.

Second, Section 702 is about national security, and no matter what precisely that means, there also is agreement that the government has greater authority in this area than it does in other areas domestically.[258]

[255] Aaron, supra note 22. The House Permanent Select Committee on Intelligence assessed this could restrict by 90% those who could authorize queries. See Marquis & Reynolds, supra note 21.

[256] See generally Marquis & Reynolds, supra note 21. Under the reauthorization, the FISC must appoint an amicus in hearings involving Section 702 unless it finds such appointment inappropriate. See Reforming Intelligence and Securing America Act § 5(b).

[257] See Aaron, supra note 22; Chauvin, supra note 22.

[258] To read through all the materials around Section 702, it seems a majority in Congress believes there is some sort of national security or foreign intelligence exception to the Fourth Amendment's warrant requirement. The point itself is hardly evident. In a case involving a domestic security threat, the Supreme Court required a warrant before using a wiretap on an American, saying, "These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government

As the debates over COINTELPRO, Total Information Awareness, and the Section 215 Program make clear, Congress would not be supportive of this sort of examination of Americans' communications, except in the context of the proven efficacy of a national security program.[259]

Finally, even in the face of ongoing disagreement about what safeguards and limits should be in place, and particularly over whether there should be a warrant required before searching Americans' Section 702 data, by universal consensus the Section 702 Program has restrictions that put domestic data gathering to absolute shame. Even before the latest reforms, court orders were required at least in predicated investigations, and use of the material in court without such orders was prohibited absent

as neutral and disinterested magistrates." United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 316–17 (1972). The Foreign Intelligence Surveillance Court of Review ruled in *In re Directives* that "a foreign intelligence exception to the warrant requirement exists," but once again that ruling was about "surveillances conducted to obtain foreign intelligence for national security purposes when those surveillances are directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." See In re Directives [redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1008–09 (FISA Ct. Rev. 2008). That is not the same as the collection of Americans' communications. The Second Circuit's ruling in *United States v. Hasbajrami* suggested the collection of USP data may be fine, but warrantless querying distinctly is not. 945 F.3d 641, 646 (2d Cir. 2019). Its ruling on this point was stark and (in our view) consistent with the correct understanding of the Fourth Amendment: "To permit that information to be accessed indiscriminately, for domestic law enforcement purposes, without any reason to believe that the individual is involved in any criminal activity . . . would be at odds with the bedrock Fourth Amendment concept that law enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search." Id. at 672. Of course, the FISC disagreed, as did one lower federal court. See id. at 673 n.21 (referencing In re DNI/AG 702(h) Certifications 2018, 941 F.3d 547 (FISA Ct. Rev. 2019)); id. at 670 (citing United States v. Mohamud, No. 10-cr-00475, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420 (9th Cir. 2016)). The Second Circuit did not find the district court's "logic persuasive" and wrote off the FISC entirely: "[E]ven to the extent that their approach differs from ours, they are not binding on this Court." Id. at 670, 673 n.21.

[259] See also A Conversation with Assistant Attorney General Matthew Olsen on the Reauthorization of FISA Section 702, Brookings Inst. (Feb. 28, 2023), https://www.brookings.edu/events/a-conversation-with-assistant-attorney-general-matthew-olsen-on-the-reauthorization-of-fisa-section-702/ [https://perma.cc/YBN9-JCTF] ("What keeps me up at night is thinking about what's going to happen if we do not renew Section 702 of the Foreign Intelligence Surveillance Act. . . . [I]f 702 expires or is watered down, the United States will lose absolutely critical insights that we need to protect the country. . . . And there are strict limits on handling any information that is incidentally collected about U.S. persons."); 164 Cong. Rec. H145 (daily ed. Jan. 11, 2018) (statement of Rep. Robert Goodlatte) ("I would have preferred to include additional reforms, but I cannot stress to my colleagues enough that our choice cannot be between a perfect reform bill and expiration of this program. The 702 program is far too important for that.").

the Attorney General's permission in major cases. Taken together, these existing and new rules may be deeply imperfect—we are in the camp that a warrant is required (absent exigency) before Americans' Section 702 data is searched—but they far exceed anything provided to constrain domestic law enforcement.[260] As defenders and opponents of Section 702 agree, multiple levels of review by all branches of government cabin Section 702 authority.[261] Again, the level of noncompliance suggests this still is not enough, but the point about constant scrutiny surely is. As a report by the Inspector General of the Department of Justice made clear, numerous lawyers review the work of the intelligence agencies for compliance with—and deviations from—existing rules.[262] And all three branches regularly conduct reviews. Nothing remotely like this occurs in the domestic sphere.

H. Putting It All Together: The Rules of Data Surveillance

This history reveals what, over a long period of time, Congress has ruled in and out regarding data surveillance. To reiterate, these are the cases in which Congress has acted, not those in which it has not acted, or not acted yet—as, for example, regarding the purchase of data from data brokers by policing agencies. When it has acted, however, Congress has been fairly clear and consistent—over a long period of time and in many varied instances—regarding a very basic set of rules. These include:

[260] It has been said that there have not been abuses of the system, but we now know that is not the case. Compare 164 Cong. Rec. H142 (daily ed. Jan. 11, 2018) (statement of Rep. Christopher Stewart) (asserting that "there has never been a known, intentional abuse of [Section 702] authority"), with PCLOB 2023 702 Report, supra note 225, at 137–38 (detailing intentional misuses of queries by FBI and NSA officials to seek information on potential tenants, dating partners, and an individual employed by opposing counsel in a non-national security criminal prosecution).

[261] See 164 Cong. Rec. H142 (daily ed. Jan. 11, 2018) (statement of Rep. Christopher Stewart) (remarking that Section 702 is "[s]ubject to multiple layers of oversight by all three branches of government"); 115 Cong. Rec. H158 (daily ed. Jan. 11, 2018) (statement of Rep. Jim Himes) ("[P]rotections exist. There are strict processes and procedures in place at the FBI as to how exactly U.S.-person information can be queried and used. On top of that, the entire 702 program is reviewed by the Foreign Intelligence Surveillance Court, the PCLOB, and is subject to meaningful congressional oversight by each and every one of us.").

[262] See Off. of the Inspector Gen., Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters 6 (2022) (noting the 100-plus lawyers who work at the DOJ's National Security Division and oversee the FBI's compliance with laws, policies, and procedures).

1. There should be transparency regarding the sorts of data surveillance in which the government is engaged;
2. Data surveillance should be authorized legislatively;
3. Data on U.S. persons should not be collected indiscriminately;
4. Data surveillance should occur only when the surveillance system is shown to be effective;
5. There should be guardrails on the collection and use of personal data, such as minimization requirements and protections against the handling of data related to the exercise of First Amendment activity;
6. Access to data about a particular individual should be predicated on some sort of suspicion regarding that person, such as reasonable articulable suspicion;
7. When possible, courts—rather than executive officials—should determine the existence of the alleged predicate;
8. Any exceptions to these rules should occur only in the realm of national security; and
9. Any data surveillance program must be constitutional.

To be clear, there are open questions. For example, although Congress has never sanctioned indiscriminate data collection of Americans, it has never considered an elaborate regulatory scheme under which it might be tenable.

III. ADDRESSING INDISCRIMINATE DATA SURVEILLANCE

What does not appear open to question is how all this ought to apply to the unregulated indiscriminate collection of personal data by federal, state, and local policing agencies when only domestic law enforcement is involved. Part I made clear the breathtaking extent to which such collection is occurring. Part II demonstrated how such collection violates the most basic rules, which Congress has insisted upon time and again, often stating the rules in terms of rule-of-law considerations or constitutional norms. When Congress has faced disagreement, it typically has been around national security, which is not implicated for the most part in domestic policing, and certainly not by the vast, vast majority of state and local policing.

Part III turns to prescription. Section III.A details the extent to which the domestic collection of innocent Americans' data violates these norms and explains what is required, at a minimum, to ensure domestic policing

agencies are acting consistently with these norms. Section III.B recognizes the public choice barriers to legislative action in this area and offers three routes to bringing minimal regulation to indiscriminate data surveillance.

A. Addressing the Lawlessness of Indiscriminate Data Surveillance

It is not clear that the Constitution permits law enforcement agencies to collect data indiscriminately and in bulk from Americans for criminal law enforcement.[263] But even if such collection is constitutional, agencies certainly should not be able to do it by engaging in evasion to escape regulation, when regulation is exactly what is required. Here, we tie the strands of Part I and Part II together by explaining how indiscriminate data surveillance by federal, state, and local agencies is slipping the bonds of congressionally recognized norms in fundamental ways, and what should be done to address it.

1. Transparency

As Part II made clear, Congress has stressed the importance of transparency repeatedly.[264] That was made clear most recently in the 2024

[263] The real stumbling block here is the Supreme Court's decision in *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000) (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995)) (prohibiting "special needs" suspicionless searching for the purposes of ordinary law enforcement); see Friedman, supra note 27, at 1189–90 (highlighting the bar imposed by *Edmond* on collecting information on individuals suspected of nothing, for law enforcement purposes).

[264] The PCLOB's initial recommendations about Section 702 leaned heavily on transparency precisely so democratic decision-makers in Congress could reach an informed decision. PCLOB 2014 702 Report, supra note 220, at 104 ("[A] number of the Board's recommendations are motivated by a desire to provide more clarity and transparency regarding the government's activities in the Section 702 program."). The history of Section 702 has been one of increasing transparency, mandated by Congress and followed by the ODNI, the latter of which gradually realized that policymakers would refuse to operate in an information vacuum. See FISA Amendments Reauthorization Act of 2017, Pub. L. No.115-118, 132 Stat. 3 (2018) (codified at 50 U.S.C. § 1801) (expanding privacy safeguards under FISA); see also Off. of the Dir. of Nat'l Intel., Statistical Transparency Report: Regarding the Use of National Security Authorities: Calendar Year 2018, at 16 (2019) (describing increased reporting requirements for the FBI under Section 702). And not infrequently, when collection becomes transparent, Congress stops it, as the fate of Section 215 and the NSA's Total Information Awareness programs make clear. That is the point of transparency: so democratically accountable decision-makers (and the polity to whom they are accountable) can make reasoned decisions. See, e.g., ACLU v. Clapper, 785 F.3d 787, 820 (2d Cir. 2015) ("Congress cannot reasonably be said to have ratified a program of which many members of Congress—and all members of the public—were not aware.").

reauthorization of Section 702.[265] Compelling reasons support transparency: it is impossible to govern what one does not know about. Yet, as detailed in Part I, policing agencies and their private partners are engaging in a variety of evasive tactics to ensure that we do not know what personal data is being collected and how it is used. This should be a red flag that democratic governance of the actions of these agencies has become impossible.

It is not going to be easy to achieve transparency when law enforcement seems determined to defeat it, and it will require a variety of approaches to tackle the problem. There is much to be said for freedom of information laws, which have been critical in allowing watchdogs to reveal what goes on domestically.[266] Law enforcement exceptions in the Privacy Act of 1974 and elsewhere have long needed trimming, and now seems an appropriate time for Congress to take up the very issue it abandoned following adoption of the Privacy Act.[267] Congress has tried to enhance sunlight even in the area of national security, such as by vesting the FISC or House and Senate intelligence committees with oversight.[268] Those efforts have not exactly failed, but they have not proven to be enough. In its 2023 report, the PCLOB repeatedly underscored the failures of transparency on critical questions and several of its recommendations to Congress were for Congress or the Intelligence Community to improve this state of affairs.[269] The Section 215 Program fiasco shows how inadequate the FISC has been as an oversight entity, and it is not clear it is markedly better now with independent amici assigned to represent the public.[270]

[265] See supra note 256.

[266] See, e.g., Shenkman et al., supra note 32, at 42–43 (relying on open records requests to obtain data regarding contractual arrangements by which federal agencies acquire data from brokers).

[267] See supra note 115 and accompanying text.

[268] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1805, 1842, 1861. The judiciary committees also have some oversight authority. See, e.g., 50 U.S.C. § 1881f(a).

[269] See PCLOB 2023 702 Report, supra note 225, at 209, 212, 220. For complaints about a lack of critical information largely around U.S. person queries, see, for example, id. at 10, 114, 180, 188–89.

[270] See, e.g., Chris Baumohl, Reforming 702: Strengthening FISA Amici, Elec. Priv. Info. Ctr. (Mar. 2, 2023), https://epic.org/reforming-702-strengthening-fisa-amici/ [https://perma.cc/DMC6-URJ8] ("While amici have been incorporated into FISA Court review on a limited basis, they continue to have a narrowly circumscribed role and lack authority to truly advocate on behalf of the public, severely limiting their value."); PCLOB 2023 702 Report, supra note 225, at 13–14 (identifying needed reforms to make the role of amici effective).

Inspectors General can force transparency and oversight. Despite the safeguards of the 2015 USA FREEDOM Act, the DOJ's Inspector General reported in 2019 that AT&T seems to have continued its cooperation with the DEA's Hemisphere operation, a fact Attorney General Merrick Garland recently confirmed.[271] But most of the country's 18,000 policing agencies do not have an effective auditor or inspector general, though when they do it often makes a difference.[272]

Because achieving transparency is difficult, and because public-private partners flagrantly flaunt the norms of transparency, even to the extent of deceiving legislators and courts, consequences are essential. Procurement regulations should outlaw secrecy requirements in MOUs and NDAs. When private partners try to force law enforcement officials to agree to secrecy nonetheless, jurisdictions should bar those vendors from obtaining contracts in that jurisdiction. This sort of ban would eliminate the incentive to secrecy in the first place. Policing officials who engage in these shenanigans should be called to the carpet and face consequences, including dismissal. When secret public-private partnerships are discovered, their funding should be terminated, as Congress did when it defunded Admiral John Poindexter's audacious TIA program and shuttered his office a year after it started (although several projects secretly continued through private contractors).[273] The message should go out that hiding mass intrusions into blameless people's lives will not be tolerated.

2. Authorization

As was clear in Part II, no one—but no one—thought bulk, indiscriminate surveillance by domestic agencies was appropriate without

[271] See supra notes 50–53 and accompanying text.

[272] See, e.g., Faiza Patel & Ivey Dyson, The NYPD Inspector General Needs Shoring Up, Brennan Ctr. for Just. (May 10, 2023), https://www.brennancenter.org/our-work/analysis-opinion/nypd-inspector-general-needs-shoring [https://perma.cc/3YJ2-U6C4] (arguing that the NYPD Inspector General's Office conducted valuable investigations and published reports on NYPD practices, which triggered important reforms in its early years, but that its recent work has been ineffective); Leila Miller, LAPD Will End Controversial Program That Aimed to Predict Where Crimes Would Occur, L.A. Times (Apr. 21, 2020, 6:17 PM), https://www.latimes.com/california/story/2020-04-21/lapd-ends-predictive-policing-program [https://perma.cc/K2VP-PURT] (stating that the LAPD made changes "seven months after the LAPD inspector general said he couldn't determine [predictive policing's] effectiveness in reducing crime").

[273] Chalmers Johnson, Dismantling the Empire: America's Last Best Hope 104–05 (2010); Wired Staff, U.S. Still Mining Data, Wired (Feb. 23, 2004, 11:00 AM), https://www.wired.com/2004/02/u-s-still-mining-terror-data/ [https://perma.cc/V3ZV-MMTL].

legislative authorization, not for any of the examples we reviewed. This, after all, is the first principle of agency government: that unauthorized activity is *ultra vires* and unconstitutional.[274] When members of Congress (and their constituents) confronted indiscriminate bulk collection, people were simply aghast. Congress shut such programs down. Yet, for much of the domestic public-private data collection set out in Part I, authorization either is absent or dubious. By definition, these programs cannot for the most part have been authorized, or we would know about them in some way other than through the work of enterprising investigative journalists and researchers. If indiscriminate data collection truly were authorized, it would not be a game of cat-and-mouse to know about it.

Agencies may argue that the indiscriminate data collection efforts described in Part I fall within the general language of their charters or organic statutes, but this argument does not work now, even if it might have more than fifty years ago. First, it simply was beyond the ken of most lawmakers at the time those statutes were adopted—often many decades, if not a half-century or century before—to imagine the technology that would allow indiscriminate bulk data surveillance. But second, and more consequentially, the claim would have to be that in authorizing agencies in general language to "enforce the law," lawmakers actually *intended* and provided for policing agencies to collect dossiers on anyone and everyone—including people for whom there is no suspicion or reason to amass data.[275] That is a tough pill to swallow, and would seem then to allow agencies to do virtually anything they chose under these general charters.

Engage in a thought experiment: imagine whether the Framers of the Constitution—or the public at that time, deeply distrustful of monarchical and overweening authority—would have countenanced indiscriminate

[274] See, e.g., INS v. Chadha, 462 U.S. 919, 953 n.16 (1983) ("[T]he Executive's administration of the laws . . . cannot reach beyond the limits of the statute that created it."); Sandra M. Stevenson, Antieau on Local Government Law § 26.15 (2d ed. 2008) ("Rules and regulations adopted by local government administrative bodies must be authorized by state constitutions, statutes, local charters, or local legislation, and when not so authorized they are held to be void."); see also La. Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986) ("[A]n agency literally has no power to act . . . unless and until Congress confers power upon it.").

[275] Barry Friedman & Maria Ponomarenko, Democratic Policing, 90 N.Y.U. L. Rev. 1827, 1884, 1894 (2015) (discussing general authorizing language of most agencies).

surveillance of their most intimate lives.[276] Their objection to writs of assistance animated the adoption of the Fourth Amendment.[277] The problem with writs of assistance—a form of reviled general warrants—was precisely that they allowed enforcement officials to search without suspicion.[278] That was Representative Nadler's point when he called the telephone metadata bulk collection "the contemporary equivalent of the British writs of assistance that early American revolutionaries opposed and that the Fourth Amendment was drafted to outlaw."[279] That was why the Second Circuit held in *United States v. Hasbajrami* that the use of the Section 702 data by the FBI resembled a "general warrant."[280] Both members of Congress and federal judges believed that the more indiscriminate the collection of personal data—not based on suspicion of any wronging—the more it crossed a constitutional line.

Even if indiscriminate data collection is constitutional, there is no way that this sort of bulk collection of personal data should be permitted—or approved in any way by a court—without the clearest of legislative authorization. As the Second Circuit said in *ACLU v. Clapper* about the 215 Program, had Congress chosen "to authorize such a far-reaching and unprecedented program, it ha[d] every opportunity to do so, and to do so unambiguously."[281] That ought to be the standard, and yet at present, rather than unambiguous authorization, there typically is none.

3. Legitimate Law Enforcement Purpose and Efficacy

It's not enough that formal statutory authorization exists; there has to be a legitimate governmental purpose actually furthered by whatever law enforcement does. Obviously, law enforcement officials cannot dip into massive pools of personal data to spy on romantic interests, a

[276] David Gray, The Fourth Amendment in an Age of Surveillance 76 (2017) (citing Goldman v. United States, 316 U.S. 129, 139 (1940) (Murphy, J., dissenting)); David Gray & Danielle Keats Citron, The Right to Quantitative Privacy, 98 Minn. L. Rev. 62, 70 (2013) (explaining that the Fourth Amendment responded to abuses of general warrants, including writs of assistance, in "subject[ing] our forefathers to the eighteenth-century equivalent of a surveillance state").

[277] Gray, supra note 276, at 140; Brief for Scholars of the History and Meaning of the Fourth Amendment as Amici Curiae Supporting Petitioner at 7, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

[278] Gray, supra note 276, at 18 (citing Wilkes v. Wood, 98 Eng. Rep. 489, 498 (C.P. 1763)).

[279] 161 Cong. Rec. 6616 (daily ed. May 13, 2015).

[280] United States v. Hasbajrami, 945 F.3d 641, 671 (2d Cir. 2019).

[281] ACLU v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015).

phenomenon so common that it has a name: LOVEINT.[282] But in light of the potential harms associated with mass data public-private partnerships, it is untenable that these programs exist in the absence of a systematized showing of efficacy. If data is required to establish such efficacy, then carefully controlled pilot programs are the answer.

Efficacy of policing agency practices is an issue that does not receive nearly the attention it deserves, but when attention is paid it makes a difference. One reason the Section 215 Program was halted, while the Section 702 Program was continued, surely related to the programs' differing efficacy. After all, each program collected personal data of Americans, and the data collected by the Section 702 Program was far more revealing. With regard to Section 702, however, defenders and detractors alike saw the general utility of the program.[283] With the Section 215 Program, by contrast, there was skepticism that it was accomplishing much of anything, making it difficult to justify the huge intrusion on privacy and threat of government misuse of the data.[284] And when Section 702 was up for reauthorization in 2023, the PCLOB—while generally laudatory of the intelligence value of the program—questioned whether the same efficacy exists with regard to queries of U.S. persons, especially for purely criminal (i.e., not national security) purposes.[285]

Some showing of efficacy might be required as a matter of constitutional law. It is basic constitutional law that government bodies

[282] See Selyukh, supra note 63 (describing practice of NSA employees caught using government surveillance tools to spy on emails and phone calls of current and former spouses and lovers).

[283] See PCLOB 2014 702 Report, supra note 220, at 104. This was evident once again around the 2024 reauthorization of Section 702 of FISA. Marquis & Reynolds, supra note 21 (noting that despite differences in policy views, "there is often broad agreement about Section 702's inherent national security value").

[284] See, e.g., PCLOB Report, supra note 189, at 13 ("Any governmental program that entails such costs requires a strong showing of efficacy. We do not believe the NSA's telephone records program conducted under Section 215 meets that standard."); Franklin, supra note 186 (describing the new Section 215 "call detail records" program as "no more valuable than the ineffective former bulk collection program that it replaced"); President's Review Group Report, supra note 237, at 104 ("Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.").

[285] See PCLOB 2023 702 Report, supra note 225, at 189 (suggesting that the FBI "may not need [this] authority").

cannot act without a legitimate public purpose.[286] And when the countervailing considerations are significant enough, that purpose not only has to be "compelling," but has to be shown to work.[287] Whether strict scrutiny should apply to indiscriminate data collection is an open question, but at the least there must be some clear showing of public purpose.[288] Due to the lack of transparency and authorization, however, we have no idea the actual purpose for which much of the data is being acquired today, let alone whether it works. For what it is worth, the recent ODNI Report suggests the government itself cannot answer this question.[289]

Even putting constitutional law to one side, requiring some showing of efficacy is unquestionably good policy. It's a basic (and obvious) principle of cost-benefit analysis that if you can't show a benefit, then you don't even have to worry about assessing the costs.[290] In the fight over Section 215, the most detailed evaluation of the relevant calculus was by the President's Review Group ("PRG"). The PRG pointed out "there is always a possibility that acquisition of more information . . . might ultimately prove helpful."[291] But it discounted this, saying, "that abstract possibility does not, by itself, provide a sufficient justification for acquiring more information."[292] Pointing to the familiar harms to liberty,

[286] See Ronald D. Rotunda, John E. Nowak & J. Nelson Young, Treatise on Constitutional Law: Substance and Procedure 324 (1986) (arguing that, under "rational relationship" test, law must have a rational relationship to an "end of government which is not prohibited by the Constitution").

[287] See id. (suggesting that the "strict scrutiny" test requires that the law "show a close relationship" to a "compelling" or "overriding" government interest).

[288] See Friedman, supra note 27, at 1147 (holding that articulable and legitimate government purpose is a constitutional prerequisite of government data collection applied to digital surveillance). See, e.g., Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 207–09 (1946) (stating that no subpoena can call for documents so broadly or indefinitely that it approaches the character of a general warrant); Hale v. Henkel, 201 U.S. 43, 76–77 (1906) (invalidating subpoena as unreasonable because it was too sweeping and unnecessary to any potential criminal prosecution); Shapiro v. United States, 335 U.S. 1, 30–33 (1948) (suggesting that the government can subpoena records that an individual was required to maintain but cannot require turning over data if it is irrelevant to any lawful purpose).

[289] See ODNI Report, supra note 23, at 21. ("But the IC does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements. Accordingly, our first recommendation is for the IC to implement a process that affords it better insight, on a going-forward basis, as to that acquisition and use.").

[290] See Steve Aos, What Is the Bottom Line?, 14 Criminology & Pub. Pol'y 633, 634 (2015) (stating that if no discernible benefits are found after initial review, then costs are irrelevant).

[291] President's Review Group Report, supra note 237, at 51.

[292] Id.

privacy, and overweening government power, it concluded that the 215 Program should be shut down.[293] And it was. The PCLOB deemed proof of efficacy to be sufficiently critical to a sound national security that it recommended that "[t]he government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs."[294] "Without such determinations, policymakers and courts cannot effectively weigh the interests of the government in conducting a program against the intrusions on privacy and civil liberties that it may cause."[295] As the PCLOB also noted, "counterterrorism resources are not unlimited," and those limited resources should be deployed sensibly.[296] The same is true of law enforcement resources more generally, yet the massive data grab in progress is both expensive and labor intensive in terms of using the technology and data and running down leads. Even Rachel Brand, a PCLOB member who dissented from some of its conclusions regarding the 215 Program, nonetheless stressed how important it was to evaluate efficacy.[297] Recognizing the "dangerous" privacy violations that could occur "[w]henever the government possesses large amounts of information," she insisted that in the "short term . . . the government should frequently assess whether it continues to provide the potential benefits it is currently believed to have, including whether the incremental benefit provided by the program is eroded by the development of additional investigative tools."[298] Further, she stressed, this should not be some off-the-cuff determination, but a "formalized" evaluation, "conducted at regular intervals with involvement by this Board, approved by officials at the highest levels of the Executive Branch, and briefed to the Intelligence and Judiciary Committees."[299]

There's every reason to be skeptical of the efficacy of the massive indiscriminate data surveillance now afoot. Due to the lack of transparency and authorization, we have little or no idea about the actual

[293] Id. at 17.

[294] PCLOB 2014 702 Report, supra note 220, at 13. The PCLOB repeated this recommendation in its 2023 report. See PCLOB 2023 702 Report, supra note 225, at 15 ("Recommendation 19: The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.").

[295] PCLOB 2014 702 Report, supra note 220, at 148.

[296] Id.

[297] See PCLOB Report, supra note 189, at 211–13.

[298] Id. at 211, 213.

[299] Id. at 213.

purpose(s) for which much of the data is being acquired today, let alone whether those programs serve the ostensible purposes. Some of the collection seems meant for predictive policing purposes. Studies have shown some limited value to "location-based" predictive algorithms, i.e., identifying crime hot spots, though there are studies to the contrary as well.[300] On the other hand, "person-based" predictive policing has almost always failed, and been criticized widely.[301] Yet, apparently agencies still are acquiring data for this purpose.[302] The other reason to collect the data is post hoc crime investigation. This was the government's argument for the propriety of the Section 215 program.[303] This is the proverbial needle just waiting in the haystack for the day it is needed. Of course, collecting everyone's data in a suspicionless way to further criminal law investigations is the justification most likely to run afoul of the Supreme Court's "special needs" jurisprudence, which holds that generalized searching is inappropriate to further the purposes of ordinary law enforcement.[304] In any event, without requiring a showing of efficacy, no one has the information to determine whether data collection is valuable at all.

[300] See, e.g., L.A. Off. of the Inspector Gen., Review of Selected Los Angeles Police Department Data-Driven Policing Strategies 25–30 (Mar. 8, 2019), https://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf [https://perma.cc/G3KG-6ARP] (stating that the impact of Los Angeles' PredPol program, designed to predict where and when crimes will most likely occur, is difficult to determine and limited by the fact that most PredPol visits to given locations are very short; earlier study found crime almost twice as likely to occur in locations selected by the PredPol algorithm than in locations selected by crime analysts).

[301] Id. at 14. See, e.g., Jessica Saunders, Priscillia Hunt & John S. Hollywood, Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot, 12 J. Experimental Criminology 347, 363 (2016) (arguing that the Chicago Police Department's use of a "Strategic Subjects List" of people estimated to be at highest risk of gun violence did not make meaningful impact on crime). As computer scientist Arvind Narayanan explains, the claim that algorithms can predict criminal activity is "[f]undamentally dubious" "snake oil." Arvind Narayanan, How to Recognize AI Snake Oil 5, 9 (unpublished manuscript), https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf [https://perma.cc/83D3-DB6B] (last visited May 16, 2024).

[302] See, e.g., Saunders et al., supra note 301 (discussing the Chicago Police Department's use of "Strategic Subjects List" of people estimated to be at highest risk of gun violence); Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 34–83 (2017) (discussing police use of predictive technologies); Jens Ludwig & Sendhil Mullainathan, Fragile Algorithms and Fallible Decision-Makers: Lessons from the Justice System, 35 J. Econ. Persps. 71, 72–73 (2021), https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.35.4.71 [https://perma.cc/L6MC-24AU] (discussing application of artificial intelligence and predictive policing in the criminal justice system).

[303] See supra notes 186–87 and accompanying text.

[304] See supra note 263.

At some point, of course, total information awareness *would* be useful. It obviously would make law enforcement's job easier if each of us had a tracking chip installed in our arms, so that our location was available and known at all times. It is hard to imagine any legislative support for this sort of program, though, let alone public or judicial approval. That seems to be the lesson from the prompt rejection of Total Information Awareness.[305] So vendors are selling what, if one is candid, are second (or third) best solutions. Law enforcement can't overtly get all of your data, so vendors sell them bits and pieces. If the desire is to get partial information on all our whereabouts and doings, then in addition to transparency and authorization, some showing of efficacy is essential.

4. Strict Regulation

In the congressional discussions in Part II, public actors repeatedly identified two sorts of harms from indiscriminate collection of personal data in bulk. First, there were tangible and intangible harms, most notably the blow to privacy, security, and free expression, often falling most frequently on marginalized communities or people pushing for social change. Second, there was the concern about the overweening power accruing to government from the possession of this sort of totalizing information—the very thing Total Information Awareness's all-seeing eye logo underscored. It is precisely because of the grave threats that can follow from the massive collection of personal data, that even if a legislative body is ready to authorize it, there still must be strict regulation of the collection, storage, retention, use, and sharing of the data.

Because the very nature of indiscriminate bulk collection is its lack of front-end control, restrictions on back-end access and use are essential.[306] And yet again, they, for the most part, are lacking in the current data-grab environment. This Subsection now describes and elaborates upon the sorts of back-end controls Congress has indicated are essential.

[305] Sayaka Kawakami & Sarah C. McCarty, Privacy Year in Review: Privacy Impact Assessments, Airline Passenger Pre-Screening, and Government Data Mining, 1 I/S J.L. & Pol'y 219, 249 (2005).

[306] See PCLOB 2014 702 Report, supra note 220, at 153 (separate statement of Chairman David Medine and Board Member Patricia Wald) ("Since Section 702 does not require any particularized judicial finding to support the initial collection of information . . . further safeguards should be required to limit the permissible scope of U.S. person queries.").

a. Predicates and Review

The first and most important limitation on access and use must be some predicate to control it. There must be rules for the level of suspicion required to search the data, and whose permission must be sought. When law enforcement wants to search for sensitive, personal information about someone, it often must get a warrant. And whether a warrant is required or not, they must have a legal predicate like probable cause.[307] Probable cause is a justification for searching for personal information that explains why this person, out of all people, deserves to have their information accessed by law enforcement officials. A warrant is a determination by a neutral official, not caught up in the law enforcement mission, that the intrusion is justified.[308]

As the debate over Section 215 made clear, no one thought unjustified access to data was permissible. There had to be a basis—a reason—to search personal data. In the debate over Section 215, not a single person advocated access without a reasonable suspicion predicate being met: the only discussion was on who would sign off on it. Predicates are built into the FISA statute itself, which requires a showing that a selector is tied to a foreign intelligence purpose or a crime. The FBI was chastised for approving batch queries of the 702 data without indicating tailored predicates for particular searches.[309]

For the most part, congressional and executive branch understanding was that agency officials should not decide on their own if there is enough of a predicate to justify a search. With regard to Section 215, President Obama pressed for the FISC to approve selectors, even before Congress decided what to do with the program.[310] Congress then wrote that requirement for judicial sign-off on reasonable suspicion into law.[311]

[307] See Illinois v. Gates, 462 U.S. 213, 214 (1983) (establishing a "totality of the circumstances" approach to determining whether there was probable cause for a warrant authorizing search).

[308] See Friedman, supra note 151, at 241 (describing access to third-party information via warrantless subpoena as a "license to pry").

[309] See Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities 26 (Apr. 2022) [hereinafter ASTR 2021], https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf [https://perma.cc/P3P9-L2G7] (identifying instances in which a FISC order was required pursuant to Section 702 but not obtained); Goitein, supra note 247 ("The FBI also engages in 'batch queries,' querying thousands or even tens of thousands of Americans' communications at one time using a single justification.").

[310] White House Office of the Press Secretary, supra note 195.

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

Section 702 remains an anomaly because FBI analysts can conduct searches of the data on their own before the commencement of a predicated investigation.[312] As indicated by the tie vote in the House of Representatives over the 2024 reauthorization, substantial numbers of members of Congress believe a warrant should be required before Americans' data is queried.[313] As Senator Dick Durbin emphasized in voting against reauthorization, "If the government wants to spy on my private communications or the private communications of any American, they should be required to get approval from a judge, just as our Founding Fathers intended in writing the Constitution."[314] However, even without a warrant requirement, a predicate must be possessed and recorded.[315] Nonetheless, this authority remains controversial.[316]

When police gather and hold data on their own, policing officials can search their databases at will, with no predicate whatsoever. This alone might be a reason to ban law enforcement from collecting and holding personal data. That was the decision Congress made in the USA

[312] While data is only added to the FBI's Section 702 database if it "pertains to open, fully predicated national security investigations," once in the database, FBI analysts routinely search that data at earlier stages of unrelated, unpredicated investigations. ASTR 2022, supra note 246, at 22 (noting that the FBI has broader query authority than other intelligence agencies but only runs its queries against a subset of Section 702 targets (approximately 3.2%)); see also PCLOB 2014 702 Report, supra note 220, at 137 (noting that FBI analysts routinely search databases containing Section 702 data without reasonable suspicion).

[313] See Tarinelli, House Approves, supra note 250; Marquis & Reynolds, supra note 21 (discussing the "sweeping limitations," including a warrant requirement, included in the House Judiciary's proposal that was ultimately not adopted).

[314] NPR, supra note 21; see also Press Release, Dick Durbin, U.S. Sen., Durbin Votes Against FISA Reauthorization Bill (Apr. 20, 2024), https://www.durbin.senate.gov/newsroom/press-releases/durbin-votes-against-fisa-reauthorization-bill [https://perma.cc/AV4Y-TJVZ].

[315] FBI analysts apparently have violated this rule frequently, but noncompliance has been detected and new controls put in place. See ASTR 2021, supra note 309, at 20–22 (describing, for example, how the FBI added a new attorney approval process, affirmative "opt-in" requirements, and new enhanced approval requirements for certain sensitive queries).

[316] See Marquis & Reynolds, supra note 21 (characterizing the warrant amendment rejection as a "dramatic tie vote"). The largest controversy in the PCLOB's September 2023 report on Section 702 was over a recommendation about requiring that the government establish a predicate showing to the FISC before U.S. person data is queried. Recommendation 3 states, "Congress should require FISC authorization of U.S. person query terms" and suggests a predicate of "reasonably likely to retrieve" foreign intelligence or evidence of a crime. PCLOB 2023 702 Report, supra note 225, at 12. Writing separately, Chair Sharon Bradford Franklin argued the Constitution requires a "probable cause" standard, id. at A-2 to -3, while two members of the Board felt imposing FISC review was too burdensome and unnecessary, id. at 17. Nonetheless, those two members recommended a variety of measures to tighten and regulate queries of U.S. person data. Id. at B-49 et seq.

FREEDOM Act. Some agencies have predicates and procedures for internal sign-offs, as was happening with the Section 215 data prior to the President and Congress putting a stop to it. Yet, as the Supreme Court said in *Riley v. California*, while holding that cell phones could not be searched without a warrant, "the Founders did not fight a revolution to gain the right to government agency protocols."[317] Recognizing the problem with uncontrolled access to stored data, some agencies have begun to get one warrant to collect data, and another to access it.[318]

Yet, for the most part, no predicate seems to be required to access *any* of the data made available to law enforcement in public-private partnerships. This surely must cease.

b. Protections

It is not just predicates at issue, though; it is any sort of protections for the range of things that can—and do—go wrong with policing agency access to our private information. Virtually none of these public-private data projects involve minimization to remove information that should not be included or to delete inaccurate information. Yet, when Congress authorizes the invasive collection and access to digital data—under Title III or Section 702, for example—it requires minimization.[319] We also simply do not know if the data in many cases is "dirty"—racially biased, erroneous, or otherwise not the sort of thing law enforcement should hold.[320] We have no clue if it is being used, or could be used, in ways that intrude upon or chill First Amendment liberties.

Because the domestic collection programs we identify in Part I exist without legislative authorization, there are none of these sorts of protections against bias, dirty data, insecure storage, and the like. There

[317] 573 U.S. 373, 398 (2014).

[318] See, e.g., Thomas v. Commonwealth, No. 0613-21-3, 2022 WL 3362920, at *3, *10 (Va. Ct. App. Aug. 16, 2022) (showing how police obtained both a geofencing warrant to identify cellular devices in the vicinity of an alleged burglary and, after combing through data produced by Google, a "secondary search warrant" requesting the specific identity of an individual whose data linked him to the area of the crime at the relevant time).

[319] See 18 U.S.C. § 2518(5); 50 U.S.C. § 1801(h).

[320] See Rashida Richardson, Jason M. Schultz & Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. Online 15, 15 (2019), https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf [https://perma.cc/APS7-FWX7] (describing "dirty data" as inaccurate, skewed, systematically biased, and the result of "dirty policing").

are no fair information practice restrictions like in the Privacy Act of 1974. For instance, policing agencies are not bound by the commitment that they only collect personal data for a legitimate purpose. They are not required to use personal data only for that specific purpose. They are not precluded from sharing personal data unless doing so would be connected to the original reason for which the information was collected. They are not bound to keep personal data secure. They are not forbidden from collecting information that solely relates to First Amendment activities. They do not have to worry about racially biased data. They do not have to do privacy impact assessments for their data collection efforts. In short, policing agencies have none of the procedural safeguards provided by congressional law and norms. All this should be written into law.

5. Judicial Review

Finally, there is the topic that should need no explanation, but apparently does. Secret acquisition of data, hidden by design, evades judicial review. Yet, it is difficult to imagine a domestic data collection program that would survive constitutional scrutiny without allowing judges to weigh in. Judges who have learned that policing agencies are using surveillance technologies secretively, such as Stingrays, have condemned this in strong terms.[321] One of the more jaw-dropping provisions of the 2018 FISA reauthorization was the provision allowing the Attorney General to certify that it was appropriate to use certain information not obtained with a warrant. That provision expressly precluded judicial review.[322] If challenged, it's hard to say whether the Supreme Court might uphold that preclusion, given national security concerns. But the simple fact is that preclusion of judicial review of agency action is disfavored.[323] And it should be when constitutional rights are implicated, as they plainly are with this sort of mass data acquisition. It is difficult to imagine preclusion of judicial review being upheld by courts in the purely domestic situation.

[321] See Barry Friedman, supra note 67, at 103–05.

[322] See FISA Amendments Reauthorization Act of 2017, 50 U.S.C. § 1881e(a)(2).

[323] See Webster v. Doe, 486 U.S. 592, 603 (1988) (holding that even if statute grants agency absolute discretion precluding judicial review of the merits of agency decision, federal courts may still consider constitutional claims absent clear congressional intent to preclude such review; establishing the clear-statement rule); Stehney v. Perry, 101 F.3d 925, 934 (3d Cir. 1996) (holding that since there is no statute expressly precluding judicial review of colorable constitutional claims arising from NSA's security clearance procedure, sovereign immunity did not preclude judicial review).

At present, not only is there no judicial review, there is not even sufficient transparency in many cases to permit it. Once again, the availability of judicial review should be made clear by statute, but in any event, courts should exercise it.

B. Motivating Regulation: Of Nudges, Sunsets, and Defaults

The problem is not so much knowing what regulation should look like, as it is getting regulators—mostly legislative bodies—to do their jobs and provide the necessary regulation. Although there may be some devils in the details, nothing in Section III.A is particularly novel. It is the basics of democratic governance.

As we have seen in the struggles over national security legislation, and as many scholars have documented with regard to the regulation of domestic law enforcement, legislators often are reluctant to step up for fear they will be branded as being soft on crime or attacked for "handcuff[ing] . . . the police" if something goes wrong.[324] As President Obama pointed out when controversy erupted in the face of the Snowden revelations, when bad things happen, the questions are not about civil liberties, but why they were not prevented: "[T]he men and women at the NSA know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots."[325] What is true of the Intelligence Community and policing officials is true of legislative bodies as well, especially because in those instances

[324] The phrase refers back to charges leveled at the Warren Court by those frustrated by its criminal procedure decisions, especially *Miranda v. Arizona*, 384 U.S. 436 (1966). See More Criminals to Go Free? Effect of High Court's Ruling, U.S. News & World Rep., June 27, 1966, at 33 (quoting Los Angeles Mayor Samuel W. Yorty). It has picked up momentum since. See e.g., Stephen J. Schulhofer, Reconsidering *Miranda*, 54 U. Chi. L. Rev. 435, 454 (1987); Paul G. Cassell & Richard Fowles, Handcuffing the Cops? A Thirty-Year Perspective on *Miranda*'s Harmful Effects on Law Enforcement, 50 Stan. L. Rev. 1055, 1057 (1998); Albert W. Alschuler, Studying the Exclusionary Rule: An Empirical Classic, 75 U. Chi. L. Rev. 1365, 1374 (2008). For scholarship on the public choice challenges of regulating law enforcement, see Barry Friedman & Elizabeth G. Jánszky, Policing's Information Problem, 99 Tex. L. Rev. 1, 25 (2020); William J. Stuntz, The Political Constitution of Criminal Justice, 119 Harv. L. Rev. 780, 795 (2006); Rachel E. Barkow, Federalism and the Politics of Sentencing, 105 Colum. L. Rev. 1276, 1278–83 (2005).

[325] Press Release, White House, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [https://perma.cc/4EKT-4RFZ].

policing officials will be quick to point to legislation they believe (sincerely or tactically) kept them from doing their job.[326]

Getting legislative bodies to act is difficult, but not impossible; take legislative action around Section 215 as an example. It is not like the existence of the 215 Program was a secret at the high levels of government before Edward Snowden blew his whistle. President Obama and high-ranking executive officials obviously knew. So too did members of Congress who were read in (including the Gang of Eight and some other intelligence committee members).[327] The Second Circuit correctly concluded none of this internal knowledge qualified as democratic authorization of the program, but we cannot say that there was widespread ignorance.[328]

What finally motivated Congress to act were three things: sunshine, sunsets, and judicial decisions. As to sunshine—that is the transparency we already have covered. Salience often moves legislative bodies to act, and without transparency there is no salience.[329] As for sunsets, the existing authority for the 215 Program was going to expire, and in fact it did just before Congress passed the USA FREEDOM Act of 2015.[330] And the Second Circuit's decision holding that the program itself was unauthorized by Congress made clear nothing could continue until Congress acted affirmatively.[331]

This final Subsection addresses three approaches that could help spark democratic regulation of policing agency data collection. They are not a complete answer, but they hold out some promise. All of them rest on the

[326] Friedman & Jánszky, supra note 324, at 37–39.

[327] Alfred Cumming, Cong. Rsch. Serv., Memorandum: Statutory Procedures Under Which Congress Is to Be Informed of U.S. Intelligence Activities, Including Covert Actions 5–7 (2006).

[328] ACLU v. Clapper, 785 F.3d 787, 820–21 (2d Cir. 2015) (finding Section 215 to have been "'legislatively ratified' . . . would ignore reality" though a "limited subset of members of Congress had a comprehensive understanding of the program"); Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint at 27, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-03994) ("[A]ll Members of Congress had access to information about this program and the legal authority for it.").

[329] Friedman & Jánszky, supra note 324, at 33 ("When information about police tactics is readily available, it often becomes salient, spurring legislative and executive action.").

[330] Julian Hattem, Patriot Act Expires as Paul Blocks Final Vote on NSA Reform, The Hill (May 31, 2015, 6:41 PM), https://thehill.com/policy/national-security/243575-patriot-act-expires-as-paul-blocks-final-vote-on-NSA-reform/ [https://perma.cc/5DNP-3J8D].

[331] *Clapper*, 785 F.3d at 822–24 (finding that, since Section 215 was not authorized, the Court did not need to consider "weighty constitutional issues").

idea that legislative bodies or other regulators can be nudged—or forced—to do their job.

1. Interbranch Dialogue: Pressing One Another over the Finish Line

Scholars have noted the judicial and legislative interaction that can lead to regulation of law enforcement information gathering.[332] The adoption of FISA is an example. In part, it was motivated by the hearings of the Church Committee, but it also was fostered by the Supreme Court's decision in *United States v. United States District Court*.[333] There, the Court held that warrants were required for searches in service of domestic security.[334] The Court also provided some hints about how to proceed, such as using a "specially designated court" to preserve secrecy.[335] Hence the birth of the FISC.[336]

Perhaps the most noted case of this sort of interbranch problem solving was adoption of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the "Wiretap Act."[337] In *Katz v. United States*, the Supreme Court held that wiretapping required a warrant.[338] In *Berger v. New York*, the Court invalidated New York's wiretap law.[339] *Berger* also provided something of a roadmap for what a valid wiretap law might

[332] See, e.g., William C. Banks & M.E. Bowman, Executive Authority for National Security Surveillance, 50 Am. U. L. Rev. 1, 31–73 (2000) (describing the role of the judicial, executive, and legislative branches in national security surveillance reforms).

[333] See Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1277 (2004) ("FISA emerged as a response to the Church Committee reports and to the [*United States v. United States District Court* (Keith)] case."); Michael T. Francel, Rubber-Stamping: Legislative, Executive, and Judicial Responses to Critiques of the Foreign Intelligence Surveillance Court One Year After the 2013 NSA Leaks, 66 Admin. L. Rev. 409, 416–18 (2014) (explaining how the *Keith* case and Church Committee "provided the impetus for the enactment of FISA"); Diane Carraway Piette & Jesselyn Radack, Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall," 17 Stan. L. & Pol'y Rev. 437, 443 n.27 (2006) (same).

[334] United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 323–24 (1972).

[335] Id. at 323.

[336] See, e.g., Patricia L. Bellia, The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law, 50 Vill. L. Rev. 425, 437 (2005) ("FISA took up the Court's invitation to route requests for surveillance involving national security to a specific forum and created a special federal court for that purpose.").

[337] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–23 (codified as amended at 18 U.S.C. §§ 2510–23).

[338] 389 U.S. 347, 353, 355, 359 (1967).

[339] 388 U.S. 41, 47, 54, 64 (1967).

look like.[340] Congress took the hint in adopting Title III, but once it was motivated to legislate, it clearly stepped beyond what the Court required, just as Congress did in adopting FISA.[341]

This is precisely what courts need to do: indicate that indiscriminate data surveillance is problematic, and provide direction about what is permissible and what is not. If they do this, legislative bodies may take the hint and step up.

The problem courts face is that cases involving surveillance data collection tend to come to them in specific criminal matters. This poses a difficulty because the use of the data in any given case might be quite limited, such that the court does not have a complete picture of the broader ongoing data collection effort. And it also is a problem because courts have not always shown great courage in suppressing evidence in criminal cases.[342]

Commonwealth v. McCarthy exemplifies the problem and its solution.[343] In that case, a drug dealer was prosecuted based in part on license plate reader images showing him traveling over particular bridges to a known destination.[344] The court concluded that the defendant's Fourth Amendment rights had not been violated because all that was at issue in the case was "four cameras placed at two fixed locations" on either end of the two bridges.[345] "This limited surveillance does not allow the Commonwealth to monitor the whole of the defendant's public movements."[346] The court was unable to "say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections."[347] Still, the court stated, "With enough cameras in enough locations, the historic location data from an

[340] Id. at 47–49; see also Susan Freiwald, First Principles of Communications Privacy, 2007 Stan. Tech. L. Rev. 3, 5 (noting that the Supreme Court in *Berger* "set forth the constitutional requirements for any statute that purported to authorize law enforcement's use of electronic surveillance").

[341] See Friedman, supra note 151, at 103–05; see also Clifford S. Fishman, The "Minimization" Requirement in Electronic Surveillance: Title III, the Fourth Amendment, and the Dread *Scott* Decision, 28 Am. U. L. Rev. 315, 316 (1979) (noting that Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in part to comply with *Berger*); Peter P. Swire, *Katz* Is Dead. Long Live *Katz*, 102 Mich. L. Rev. 904, 911 (2004).

[342] Friedman, supra note 151, at 81–83, 86–91 (describing difficult incentives facing judges forced to suppress evidence in case of defendants who plainly committed the offense).

[343] 142 N.E.3d 1090, 1104, 1106 (Mass. 2020).

[344] Id. at 1096.

[345] Id. at 1106.

[346] Id.

[347] Id.

[automated license plate reader ("ALPR")] system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes."[348]

It's unfortunate that the *McCarthy* court could not or would not do more to address the problem, but the decision surely was enough of a hint to the Massachusetts legislature that something needed to be done. It is easy to see why the court was reluctant to invalidate a conviction, with so few data points revealed. What the court needed was a broader picture of the surveillance system, and a case in which its entirety could be tested. Massachusetts has since considered legislation, though it has not managed to pass it.[349] If Massachusetts does not, the Supreme Judicial Court should consider hinting more broadly that it will not allow the program without full transparency, if not authorization.

One clear thing that courts should do is relax their rules about standing in these cases, so challenges can be brought outside the context of criminal actions, and a fuller record can be developed. The *McCarthy* court indicated it was hamstrung because "the record is silent as to how many of these cameras currently exist, where they are located, and how many of them detected the defendant."[350] This is the sort of information not likely to be developed fully in a criminal prosecution. Unfortunately, in broader challenges, the government will argue challengers have no standing, and courts too often accept this.[351] That was the case with an early challenge to Section 702's authorization by Congress in 2008.[352] The government argued and the Supreme Court accepted that "it is speculative whether the Government will imminently target communications to which respondents are parties."[353] The proof sought by the Court was absent because, according to the government, the surveillance program had to be kept secret.[354] It's true that the parties had "no actual knowledge" of the government's targeting practices, but in the

[348] Id. at 1104.

[349] See H. 3404, 2023 Leg., 193d Sess. (Mass. 2023) (limiting the use of data collected by ALPRs).

[350] *McCarthy*, 142 N.E.3d at 1105.

[351] See Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013) (finding no standing for an "injury based on potential future surveillance"); see also Christopher Slobogin, Standing and Covert Surveillance, 42 Pepp. L. Rev. 517, 518 (2015) (explaining the challenges to establishing standing to challenge surveillance programs).

[352] *Clapper*, 568 U.S. at 401.

[353] Id. at 411.

[354] Id. at 412 n.4 (insisting that the burden to plead specific facts remained on plaintiffs despite the secrecy of those facts).

face of widespread surveillance programs, courts should loosen standing requirements to allow a record to develop.[355] Many states allow public interest standing, which might enable just this.[356]

When cases do manage to come before courts, the other thing they can do is decide them on statutory grounds if the constitutional questions seem challenging. In a concurring opinion in *United States v. Jones*, a four-Justice concurrence authored by Justice Alito concluded that long-term GPS tracking was unconstitutional, but it could not say precisely where the line was: "In circumstances involving dramatic technological change," "[a] legislative body is well situated to . . . draw detailed lines, and to balance privacy and public safety in a comprehensive way."[357] But legislative bodies will not always act unless forced to. As the Second Circuit's decision in the Section 215 Program case makes clear, a solution is to find data collection programs unauthorized by law, and then let legislative bodies grapple with the questions in the first instance.[358] That is what we argued at the outset should happen.[359]

The significance of proceeding on statutory grounds is that rather than barring the government from a practice entirely on constitutional grounds, which would require a constitutional amendment to reverse, a statutory ruling simply tosses the issue to a governmental body to tackle it. A constitutional challenge always remains in reserve if the decision-making body fails to regulate sufficiently.

2. Default Rules and Sunsets

If legislative bodies decide to permit mass collection of personal data—assuming doing so is constitutional—they unequivocally should impose

[355] Id. at 411.

[356] See Thomas B. Bennett, The Paradox of Exclusive State-Court Jurisdiction over Federal Claims, 105 Minn. L. Rev. 1211, 1212–15 (2021) (finding that "state courts have fashioned their own standing regimes, many of which welcome claims that do not depend on any showing of concrete injury to a plaintiff"); John DiManno, Beyond Taxpayers' Suits: Public Interest Standing in the States, 41 Conn. L. Rev. 639, 656–58 (2008) (finding state courts provide for more flexible public interest standing models).

[357] 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

[358] *Clapper*, 785 F.3d at 824 ("Because we conclude that the challenged program was not authorized by the statute on which the government bases its claim of legal authority, we need not and do not reach these weighty constitutional issues.").

[359] See supra notes 26–28 and accompanying text; see also Friedman, supra note 27, at 1147 ("Unless and until [sufficient data collection] regulation occurs, what the policing agencies of this country are doing is simply unconstitutional and must cease. Forthwith.").

sunsets on that authorization.[360] Sunsets allow legislative bodies to reconsider their decisions at a future point.[361] Sunsets force Congress to consider whether programs' benefits are worth the costs, an assessment that needs some transparency (to Congress at least), assessment of efficacy, and the costs to individuals and society.[362]

Sunsets force action, even when legislators are reluctant to discharge their responsibilities, as was clear in the case of the Section 215 Program. Ultimately, it was only the fact that the provision of the USA PATRIOT Act under which the FISC had approved data collection was about to sunset that forced Congress to act. While the FISC's dubious interpretation of the USA PATRIOT Act remained in place, the government could continue collecting data without regard to whether Congress signed off.[363] But only once the law allowing the collection was sunsetting—and in fact it did sunset right before Congress acted—were

[360] Emily Berman argues against sunsets in the counterterrorism area. See Emily Berman, The Paradox of Counterterrorism Sunset Provisions, 81 Fordham L. Rev. 1777, 1777, 1807–08 (2013). Her argument is based on the fact that with counterterrorism, passions will not cool over time, and information needed to regulate soundly will not be forthcoming, arguments we advance below. Although there is much wisdom in Berman's piece, it was written before passage of the USA FREEDOM Act, and before political pressures have gradually forced more information regarding Section 702 out of intelligence agencies. Perhaps more fundamentally, we are arguing for the use of sunsets in the domestic law enforcement area. Still, her point is taken—and we advance it repeatedly—regarding the difficulty of getting information out of policing agencies. But that simply has to stop if legislators are to do their job. Accord Principles of the Law, Policing § 14.10(b)(1) (Am. L. Inst. 2023) (recommending that governments require courts to release comprehensible data on surveillance orders); Friedman and Jánszky, supra note 324, at 33.

[361] John E. Finn, Sunset Clauses and Democratic Deliberation: Assessing the Significance of Sunset Provisions in Antiterrorism Legislation, 48 Colum. J. Transnat'l L. 442, 447–49 (2010) (explaining how sunset clauses can improve the quality of legislative decision-making).

[362] See, e.g., John Ip, Sunset Clauses and Counterterrorism Legislation, 2013 Pub. L. 74, 74 (finding that "appropriately designed sunset clauses . . . can play a useful role in the governance of legislatively conferred counterterrorism powers"); Jacob E. Gersen, Temporary Legislation, 74 U. Chi. L. Rev. 247, 248 (2007) (finding that, in some contexts, sunset provisions are "likely to provide far more advantages than drawbacks" including by providing "windows of opportunity for policymakers to incorporate a greater quantity and quality of information into legislative judgments"); Eric A. Posner & Adrian Vermeule, Accommodating Emergencies, 56 Stan. L. Rev. 605, 617, 626 (2003) (arguing for the inclusion of sunset provisions in counterterrorism legislation); Bruce Ackerman, Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism 80–83, 131–32 (2006) (same).

[363] See 161 Cong. Rec. H2914 (daily ed. May 13, 2015) (statement of Rep. Robert Goodlatte) ("Despite changes to the NSA bulk telephone metadata program announced by President Obama last year, the bulk collection of the records has not ceased and will not cease unless and until Congress acts to shut it down.").

those who would avoid the issue forced to stand up and be counted as to whether what the executive branch was doing was permissible.[364]

The history of Section 702 is another relevant example. That provision was adopted in 2008 and readopted subsequently, always subject to periodic reauthorization. As it progressed through time, further transparency was forced. Greater protections were layered on (although advocates contested their value, and in some cases reasonably so).[365] There was more of a chance to try to understand whether the provision was efficacious at all.

Of course, sunsets may prove worthless without disclosure. As noted above, Section 215 was reformed not only because of reconsideration, but because the Snowden revelations and the accompanying salience of the issue forced Congress's hand. Sunsets, it perhaps bears saying, are necessary, but not sufficient.[366]

The first value of sunsets is that they can cause reconsideration at a time that might be more dispassionate. Too often, legislation empowering law enforcement happens after some sort of tragedy. As passage of the USA PATRIOT Act after 9/11 shows, tragedy can lead to the passage of legislation that gives too much authority to law enforcement, which may need to be reeled back at a later date. Sunsets allow this reconsideration.[367]

The other value of sunsetting is that legislative bodies can reconsider the calculus that led to the original legislation, on both the cost and benefit sides. As we have pointed out repeatedly, too much of this data collection occurs without any showing of efficaciousness, despite the huge threat that it poses. Legislative bodies should build in measures for testing efficacy, and require reports that can inform them as to whether and how well any data collection effort works. And then can similarly learn from any civil liberties or racial harms that have occurred along the way.

---

[364] See 161 Cong. Rec. 8054–59 (2015); see also 161 Cong. Rec. H2920 (daily ed. May 13, 2015) (statement of Rep. Suzan DelBene) ("After the House acts today, it is up to the Senate leaders to pass these reforms or let the expiring provisions of the PATRIOT Act sunset."); 161 Cong. Rec. S3397 (daily ed. June 1, 2015) (statement of Sen. Richard Blumenthal) ("I have been dismayed by the divisions and delays that have prevented us from finally approving the USA FREEDOM Act before the existing law expires. We should move now.").

[365] See Off. of the Inspector Gen., Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters 6 (2022).

[366] Thanks to Emily Berman for this point.

[367] See Devon Ombres, NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform, 39 Seton Hall Legis. J. 27, 29, 43 (2015) (detailing the birth of a "mass surveillance infrastructure" after 9/11 and later reforms).

3. Pressures from Abroad

Ironically, pressure to modify indiscriminate data surveillance may come from abroad. Currently, European judicial decisions have caused the executive branch to alter practices under Section 702, although it is open to question whether these alterations are sufficient to address European concerns. But what seems to have gotten less attention is the extent to which those same concerns implicate domestic information gathering as well.

The United States has been under pressure to do something about Section 702 from global companies based in the United States handling data from EU citizens. The European Court of Justice ("EUCJ") twice has struck down U.S.-EU data sharing trade agreements because U.S. laws governing intelligence activities like Section 702 permit bulk collection of personal data transmitted to the United States without any chance for European citizens to access and review it and without minimum safeguards that comport with the principle of proportionality.[368] The EUCJ rejected the latest trade agreement because it provided for ombudsperson oversight that was not sufficiently independent from the executive branch and intelligence agencies.[369]

U.S. companies are currently in limbo, working with half-measures (standard contractual clauses) and dreading that the EUCJ will strike down the latest proposed EU-U.S. Data Privacy Framework. In May 2023, the European Parliament rejected the proposed framework because it failed to provide sufficient safeguards in the case of bulk data collection, including the lack of independent prior authorization, strong safeguards concerning the collection of bulk data, and restrictions on law enforcement to access such data.[370] On July 10, 2023, however, the European Commission agreed to sign off on the Data Privacy Framework.[371] No matter, the EUCJ has a mind of its own, and it may again strike down the trade agreement because Congress has yet to change the state of affairs under Section 702 to provide stronger protections

[368] See Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 90 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Schrems (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 180–81 (July 16, 2020).

[369] See *Schrems II*, C-311/18 at 195.

[370] See Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework, Eur. Parl. Doc. P9_TA0204 (2023).

[371] Clothilde Goujard & Alfred Ng, EU and US Reach a Deal to Let Data Flow Across the Atlantic, Politico (July 10, 2023), https://www.politico.eu/article/eu-signs-off-on-data-transfers-deal-with-us/ [https://perma.cc/7A27-MUW6].

against bulk collection.[372] Thus, in the political economy of things, it may be corporate America that ultimately provides the push to modify Section 702, in the hopes that it might enhance the possibility of a trade agreement that stands the test of EUCJ review.

Although the EU has been fixated on Section 702 and congressional regulation, the very same sort of problem may be present in domestic law enforcement collections. If so, perhaps the EU will turn its attention to them. And if it does, Congress is going to receive serious pressure from large multinational companies based in the United States to adopt legislation that gets all this data collection control. Congress likely has the power to do so, to the extent data brokers and their ilk are dealing on an interstate basis.[373] And perhaps it should.

CONCLUSION

As the Report from the Office of the Director of National Intelligence put it, there is today, "in a way that far fewer Americans seem to understand, and even fewer of them can avoid," a data grab of gargantuan proportions being pulled off by law enforcement agencies working in concert with private partners.[374] This data, as the ODNI Report also recognized, is deeply personal, and its collection and use present very real

[372] By Executive Order, President Biden attempted to meet the requirements set out in the EUCJ *Schrems* decisions, including limiting principles for the conduct of signals intelligence. Exec. Order No. 14,086, 87 Fed. Reg. 62283 (Oct. 7, 2022); Questions & Answers: EU-U.S. Data Privacy Framework, Eur. Comm'n (Oct. 7, 2022), https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_6045 [https://perma.cc/F2CA-24KN]; President Biden Signs Executive Order Implementing EU-U.S. Data Privacy Framework to Facilitate Cross-Border Data Transfers—Privacy Shield 2.0?, Crowell (Oct. 10, 2022), https://www.crowell.com/en/insights/client-alerts/president-biden-signs-executive-order-implementing-eu-u-s-data-privacy-framework-to-facilitate-cross-border-data-transfers-privacy-shield-2-0 [https://perma.cc/9TXW-B73D]. Yet, the 2024 Section 702 reauthorization bills did not codify the signals intelligence objectives set out in the Executive Order, let alone meet the *Schrems* rules. See Elizabeth Goitein & Noah Chauvin, The Year of Section 702 Reform, Part IV: The Government Surveillance Reform Act, Just Sec. (Nov. 7, 2023), https://www.justsecurity.org/89786/the-year-of-section-702-reform-part-iv-the-government-surveillance-reform-act/ [https://perma.cc/CJX5-KAXT] (noting that though one proposal, the Government Surveillance Reform Act of 2023, would be "the most significant surveillance reform legislation since FISA itself," it "does nothing to limit the scope of foreign intelligence surveillance").

[373] See Barry Friedman, Rachel Harmon & Farhang Heydari, The Federal Government's Role in Local Policing, 109 Va. L. Rev. 1527, 1585–86 (2023).

[374] ODNI Report, supra note 23, at 14.

threats to privacy and liberty.[375] Few understand it, in large part because it is being kept secret from them. What is occurring is lawless—it is almost entirely unregulated—and of dubious constitutionality. It is difficult to imagine that much if not most of this would be approved of if brought to a public vote.

Unregulated indiscriminate data surveillance by domestic law enforcement actions and their private helpers must cease. Much of it likely should not occur at all, and it would not if it were public and subjected to judicial scrutiny for what it is. What does occur must be subjected to tight regulation along the lines described here.

[375] Id. at 11.