LAWLESS SURVEILLANCE

BARRY FRIEDMAN*

Policing agencies in the United States are engaging in mass collection of personal data, building a vast architecture of surveillance. License plate readers collect our location information. Mobile forensics data terminals suck in the contents of cell phones during traffic stops. CCTV maps our movements. Cheap storage means most of this is kept for long periods of time—sometimes into perpetuity. Artificial intelligence makes searching and mining the data a snap. For most of us whose data is collected, stored, and mined, there is no suspicion whatsoever of wrongdoing.

This growing network of surveillance is almost entirely unregulated. It is, in short, lawless. The Fourth Amendment touches almost none of it, either because what is captured occurs in public, and so is supposedly "knowingly exposed," or because of the doctrine that shields information collected from third parties. It is unregulated by statutes because legislative bodies—when they even know about these surveillance systems—see little profit in taking on the police.

In the face of growing concern over such surveillance, this Article argues there is a constitutional solution sitting in plain view. In virtually every other instance in which personal information is collected by the government, courts require that a sound regulatory scheme be in place before information collection occurs. The rulings on the mandatory nature of regulation are remarkably similar, no matter under which clause of the Constitution collection is challenged.

This Article excavates this enormous body of precedent and applies it to the problem of government mass data collection. It argues that before the government can engage in such surveillance, there must be a regulatory scheme in place. And by changing the default rule from allowing police to collect absent legislative prohibition, to banning collection until there is legislative action, legislatures will be compelled to act (or there will be no surveillance). The Article defines what a minimally acceptable regulatory scheme for mass data collection must include and shows how it can be grounded in the Constitution.

 For their hugely helpful comments, I would like to thank Nick Bagley, Marc Blitz, Greg Brazeal, Ryan Calo, Max Carter-Oberstone, Erwin Chemerinsky, Danielle Citron, Andrew Ferguson, Jack Goldsmith, David Gray, Farhang Heydari, Annie Hudson-Price, Aziz Huq, Max Isaacs, Emma Kaufman, Orin Kerr, Katie Kinsey, Daryl Levinson, Jennifer Lynch, Michael Mannheimer, Laura Moy, Michael Pollack, Maria Ponomarenko, Margret Robb, Jason Schultz, Chris Slobogin, Vincent Southerland, Kathy Strandburg, Peter Swire, Matthew Tokson, Ari Waldman, Ben Wilen, Andrew Woods, and Jonathan Zittrain. This work was produced with generous support of the Filomen D'Agostino and Max E. Greenberg Research Fund at New York University School of Law.

INTRODUCTION

Policing agencies collect information. That is what they do. They investigate crimes—past, present, and future—aggregating bits and pieces of evidence as they go. They create databases of arrestees, convicted individuals, DNA, outstanding warrants, and locations where crimes occurred. They keep tabs on people: people suspected of being in gangs, people suspected of dealing drugs, people who are not permitted to fly on airplanes.

The question I want to take up here is whether the collection of all this data by those who police us—and particularly the way it is occurring today—is constitutional. In light of the ubiquity of these

policing practices and the permissiveness of the governing doctrine, the question might seem absurd. It's not.

Technology has made it possible for government to hoover up unfathomable amounts of information on people: their location, their habits, their expenditures and communications, their preferences.[1] Plummeting costs have made squirreling away all this data into perpetuity feasible. Search capacities and artificial intelligence have made combing through the information, collating it, and mining it, as simple as clicking a few buttons. And so, policing agencies—from the local police department to the FBI—have become packrats and voyeurs, holding on to vast stores of data about all of us, which they then can scrutinize whenever the fancy strikes them. Even though most of us have done nothing to arouse the suspicions of the law and likely never will.

Government policing agencies are not particularly clear on why they are gathering all this data, other than that they can. If pressed, they respond, "in case we have use for it later."[2] General Keith Alexander, the former head of the National Security Agency (NSA), was candid in defending the NSA's massive data grab after 9/11: "[Y]ou need the haystack to find the needle."[3] Cops you talk with all have a story about that time the stored license plate image cracked the big one, or how the local DNA database was instrumental in nabbing a serial criminal.[4] This may be true—there is some evidence it is true, but, as a matter of actual efficacy, we have little to go on beyond this sort of anecdotal evidence.[5]

Although its efficacy is uncertain, the threats to our freedoms and liberties from this gargantuan information grab are much clearer. Our lives are the haystacks in which the government indiscriminately searches for needles. Once, alarmist authors had to spin Orwellian tales of surveillance, or point to famous episodes of government spying like COINTELPRO, and struggle to persuade the skeptical that they did indeed have something to hide.[6] Now, the Supreme

---

[1] *See infra* Section I.A (elaborating on the claims in this paragraph).

[2] *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015) ("[T]he government takes the position that the metadata collected . . . are nevertheless 'relevant' because they may allow the NSA, at some unknown time in the future, . . . to identify information that *is* relevant.").

[3] J.D. Tuccille, *Why Spy on Everybody? Because "You Need the Haystack to Find the Needle," Says NSA Chief*, REASON (July 19, 2013, 2:39 PM), https://reason.com/2013/07/19/why-spy-on-everybody-because-you-need-th [https://perma.cc/REA8-G5ZX].

[4] Believe me; I talk with plenty of police.

[5] *See infra* notes 68–71 and accompanying text (discussing the utility of mass data collection).

[6] *See infra* Section I.B (discussing the harms of surveillance data collection).

Court itself has recognized the possibilities, with great clarity. In *Carpenter v. United States*, addressing cell site location information, the Chief Justice—writing for the majority—described "the seismic shifts in digital technology" that today allow the government to "achieve[] near perfect surveillance."[7] Not just in the here and now, he pointed out, but retrospectively. "[T]he Government can now travel back in time to retrace a person's whereabouts," giving "police access to a category of information otherwise unknowable."[8] And not just for criminal suspects; "this newfound tracking capacity runs against everyone."[9] Well said, and all true.

Still, the Justices are lost as to precisely what to do about the problem of invasive digital surveillance. An ever-growing literature—by scholars, journalists, policy professionals, and even judges—suggests Fourth Amendment doctrine needs to be rethought entirely.[10] The Justices notably have been reluctant to embark on this venture, no doubt because they have little clue where it will take them. Some have thrown up their hands and suggested the necessity for legislative intervention.[11] Legislative action plainly is called for, but—for reasons I explain—one hardly sees legislatures jumping to deal with the problem either.[12]

What I want to suggest here is that for all its seeming perplexity, we have the *constitutional* tools we need to begin to address the problem of government data surveillance right at our fingertips. We just need to shift our gaze a bit. Not only are those tools already immanent in the Constitution, there is nothing particularly novel about them. Outside the surveillance context, government is collecting data constantly, both in a targeted fashion about particular individuals, and more generally about all of us. An entire body of constitutional law has grown up around that data collection; if applied to the burgeoning surveillance state, it would do much to alleviate the threats such collection poses.[13] It would not be perfect, but it would be a notable improvement over where we are today.

This article excavates the relevant body of existing doctrine and applies it to digital surveillance, particularly bulk surveillance, arguing

---

[7] Carpenter v. United States, 138 S. Ct. 2206, 2218–19 (2018).

[8] *Id.* at 2218.

[9] *Id.*

[10] *See infra* notes 81–87 and accompanying text.

[11] *See, e.g.*, United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

[12] *See infra* notes 88–91 and accompanying text.

[13] *See infra* Part II (surveying this body of law governing various forms of government personal data collection).

that before such surveillance is deployed, the Constitution requires there be a sufficient regulatory framework in place. Not that regulation merely would be desirable, as many have pointed out, but that it is absolutely mandatory as a matter of constitutional law. Unless and until that regulation occurs, what the policing agencies of this country are doing is simply unconstitutional and must cease. Forthwith.

This admittedly is a big claim, but I intend to show that it rests on an impressively broad foundation of established constitutional law, albeit one courts and commentators alike have failed to take account of.[14] There are innumerable cases involving challenges to the collection of personal information by the government. Those challenges arise under many different clauses of the Bill of Rights. But all those cases share one thing in common: Over and over, courts—and especially the Supreme Court—require the very same basic regulatory prerequisites be met before information collection proceeds.

What are the constitutional prerequisites of government data collection that must be applied to digital surveillance? There are six. (1) Government must have *legislative authorization* before it can proceed to acquire, hold, and ultimately utilize our data. (2) The collection must be transparent to the public. (3) The authorization for collection has to be grounded in an *articulable and legitimate governmental purpose*. (4) The collection of our data *must further that purpose*. (5) *Guardrails are required* to *minimize over-collection* and to *avoid inappropriate use or revelation*. (6) There must be *a regularized process for acquiring the information*, be it through court order or otherwise, and *judicial review must be available* to challenge the collection, as well as the program that authorized it.[15]

If the prerequisites of the preceding paragraph are stunning in their lack of novelty, all the better. These are, after all, nothing other than the very building blocks of the Constitution's conception of the rule of law, found in some form in almost any challenge to government authority as encroaching on individual liberty. Yet, widespread government surveillance at present altogether avoids this foundational

---

[14] I argue elsewhere for democratic authorization of policing tactics, based on bedrock democratic values. *See, e.g.*, Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. Rev. 1827 (2015); Barry Friedman, Unwarranted: Policing Without Permission (2017). The argument here, by contrast, applies only to policing data collection, rests in rule of law concerns rather than democracy, and is immanent in existing constitutional doctrine. As such, my hope is it is utterly persuasive to judges. Still, that very different constitutional approaches lead to similar results shows the profound difficulty with police exceptionalism.

[15] All of this is described in Part II, *infra*, and applied to bulk data collection in Part III, *infra*.

set of regulatory prerequisites. Rather, when it comes to surveillance, almost anything goes.

In short, pervasive government surveillance is lawless at present. Using license plate readers, CCTV, domain awareness systems, DNA collection mechanisms, location tracking devices, cell phone extraction, purchased records of credit card transactions . . . the list goes on and on . . . policing agencies are accumulating vast amounts of data on us with nary a nod toward the most basic requirements of the rule of law. This is what must end.

Rather, before policing agencies engage in digital collection of our personal information, there must be a regulatory framework in place that addresses each of the six prerequisites enumerated above.

By "policing agencies," I mean any government agency that collects and uses private information to conduct surveillance or enforce the law. This includes what we traditionally think of as the police—the local department. And it of course encompasses federal agencies like the FBI or the Drug Enforcement Agency. But it also includes regulatory bodies like the SEC or state counterparts, and even school districts, to the extent those entities collect, retain, aggregate, and use personal data to monitor how we behave and that could lead to enforcement action of any sort.[16]

As to what requires regulation, it is the collection, retention, aggregation, and use of personal information by policing agencies through digital means. The focus of the discussion here will be primarily on collection, because without collection none of the rest can follow. I focus on digital collection because, to be honest, I am not entirely certain how to feel about whether this all applies to police jotting down information with stubby pencils in their notebooks and blotters. My suspicion is that back when that was primarily what intelligence gathering involved, it didn't matter a great deal, for two reasons. First, most of that activity was targeted at individuals and regulated by the familiar Fourth Amendment tools of cause and warrant. Second, until the age of digitization, most of that information was not particularly accessible for use and manipulation by police. But all that has changed in the era of bulk data collection, and so that is my primary focus.

Part I of this Article maps out the problem of digital data collection and the present failure of the Supreme Court to regulate it. I describe the extensive surveillance that is occurring and the harms of allowing it to occur in this lawless fashion, even while acknowledging

[16] *See* PRINCIPLES OF THE L.: POLICING § 1.01 (AM. L. INST., Tentative Draft No. 2, 2019) (defining policing agencies functionally in just these terms).

that there may well be value to some digital bulk data collection, if properly regulated. I explain that, as interpreted by the Supreme Court, the part of the Constitution seemingly designated to deal with this issue—the Fourth Amendment—doesn't, leaving a regulatory vacuum. And I recount the difficulties the Justices have encountered in bringing such surveillance under control: their uncertainty as to the efficacy or value of these surveillance tactics, a reluctance for this reason to rule them out entirely as a matter of constitutional law, and a seeming lack of adequate tools to get burgeoning surveillance under control.

Part II then points to the way out of the difficulties the Justices face, if they would just look to the extensive case law regarding government collection of personal data in other domains. This Part takes readers on a tour of how constitutional law deals with the many ways in which government seeks information from people. Information is, after all, the lifeblood of governance. What we will see, time and again, under one clause of the Constitution after another, is that there are certain prerequisites that must be met before government collects such personal data. These are the six prerequisites enumerated above, properly adopted by statute or some other democratically-accountable regulatory means. Yet at present, for the most part, these prerequisites are entirely lacking from the government's collection of surveillance data. One clear value of applying the prerequisites is that it solves the Justices' difficulties under existing Fourth Amendment doctrine. Before having to decide whether any given surveillance technique is constitutional, the Justices need only insist that legislative bodies authorize and regulate the surveillance in the first instance. (Constitutional review can, of course, follow.)

Part III takes those six prerequisites and explains how they would apply to government surveillance data collection. There's no magic here; this Part simply fills out what surveillance subject to the rule of law must look like as a statutory matter. Still, there are a few thorny issues to tackle, such as how specific legislative authorization need be, and what guardrails are appropriate.

Part IV then addresses the question of where in the Constitution the means to regulate digital surveillance is found. To date, most government digital surveillance is not deemed a "search" under existing Fourth Amendment doctrine, and so nothing can be done about it. So very sorry. Yet, as I explain in Part IV, once one sees the necessity of regulatory prerequisites, there are any number of constitutional hooks readily available by which surveillance could be brought within the rule of law, some arising under the Fourth Amendment and some not.

To be clear, what this Article demands is a set of statutory minima. Some may argue that tea is too weak. But one has to start somewhere. My hope is that once legislative bodies are required to regulate surveillance according to the six prerequisites, public debate and attention will lead to regulation that is both sensible and sufficient. If not, though, courts always have the capacity to find the regulations put in place by legislative bodies wanting under the Constitution. None of this will happen, however, unless and until legislative bodies are forced to act. The essential beginning is to recognize lawless surveillance for what it is, and to demand legality take its place.

I
THE SCOPE OF THE PROBLEM

A. The Breadth of Data Collection

We are building in the United States a vast architecture of surveillance. The construction of the whole system is not nearly as intentional and centralized as in places like China, Myanmar, or Russia.[17] Indeed, the diffuse and haphazard nature of what is being stitched together here may be the greatest protection for our liberties at present. We have the tools to engage in totalizing surveillance, but policing agencies often act on their own, and the databases under construction have not been stitched together. Still, what is being built is sweeping in scope and, absent regulation, portends ill for the future.

A good portion of the surveillance of the United States' population by law enforcement is the result of public-private partnerships. The data that those who police us want can be purchased, subpoenaed, or simply given to the government on an ask.[18] For example,

---

[17] *E.g.*, Hannah Beech, *Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown*, N.Y. TIMES (Mar. 12, 2021), https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html [https://perma.cc/4LWR-6YTM]; Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html [https://perma.cc/KK6U-P4QD]; Robyn Dixon, *Russia's Surveillance State Still Doesn't Match China. But Putin Is Racing to Catch up*, WASH. POST (Apr. 17, 2021, 4:00 AM), https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html [https://perma.cc/7W6N-CJT6].

[18] *See, e.g.*, 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/6VWC-Y589] (discussing law enforcement agencies' practices of purchasing cell phone location information); Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (June 27, 2014, 10:29 AM), https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-

many government agencies buy vast pools of information from companies like Thomson Reuters, whose CLEAR database is a "powerful public records technology" that holds extensive information on people's credit, and so forth, and "bring[s] all key content together to provide intelligent analytics in one environment."[19] Similarly, law enforcement increasingly gains ready access to the "lateral surveillance" we conduct on one another, such as through the sharing of video from Ring doorbells or license plate reads from Flock cameras.[20]

But the central focus of this Article is on the information policing agencies are gathering themselves—and sharing with one another. The FBI is constructing an enormous biometric database that will include DNA, facial images, iris scans, and voice and palm prints.[21] New York is one of several cities with an extensive Domain Awareness system, which collects and aggregates information from a network of over 3,000 cameras, license plate readers, and data from government databases.[22] No longer content with using state-run and regulated DNA databases, local departments have begun creating their own versions, snatching DNA in any way they can get it: from

your-digital-data [https://perma.cc/KL9N-JYQW] (cataloguing the types of consumer data that the government can obtain through subpoena). *See generally* Farhang Heydari, *The Private Role in Public Safety*, 90 GEO. WASH. L. REV. 696 (2022).

[19] *Thomson Reuters CLEAR*, THOMSON REUTERS LEGAL, https://legal.thomsonreuters.com/en/c/clear-investigation-solution [https://perma.cc/B7ZK-3E9G]; *see* Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, WASH. POST (Feb. 26, 2021, 4:55 PM), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data [https://perma.cc/BL95-CL7S] (detailing ICE's use of the CLEAR database).

[20] *See, e.g.*, Drew Harwell, *Home-Security Cameras Have Become a Fruitful Resource For Law Enforcement — And a Fatal Risk*, WASH. POST (Mar. 2, 2021, 6:00 AM), https://www.washingtonpost.com/technology/2021/03/02/ring-camera-fears [https://perma.cc/J9CE-NBSK] [hereinafter Harwell, *Home-Security*]; The Editorial Board, *Watchful Help or Harm?: Police Access Home Surveillance Cameras to Solve Crimes*, PITTSBURGH POST-GAZETTE (Sept. 30, 2019, 6:15 AM), https://www.post-gazette.com/opinion/editorials/2019/09/30/Home-surveillance-cameras-Ring-Amazon-police/stories/201909280013 [https://perma.cc/S39L-ZTQ3]; Drew Harwell, *License Plate Scanners Were Supposed to Bring Peace of Mind. Instead They Tore the Neighborhood Apart.*, WASH. POST (Oct. 22, 2021, 1:55 PM), https://www.washingtonpost.com/technology/2021/10/22/crime-suburbs-license-plate-readers [https://perma.cc/N28Q-4FCF]. *See generally Ring & Neighbors Public Safety Service: A Civil Rights & Civil Liberties Audit*, POLICING PROJECT, https://www.policingproject.org/ring [https://perma.cc/XKR5-C5P6] (describing the Policing Project tech audit of Ring's app and use by police).

[21] *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/2BSL-A6HS]; *see* Erin Murphy, *Databases, Doctrine, & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 805–10 (2010) (outlining evolution of criminal justice databases).

[22] Christopher Robbins, *Photos: Inside the NYPD's New "Domain Awareness" Surveillance HQ*, GOTHAMIST (Apr. 24, 2013), https://gothamist.com/news/photos-inside-the-nypds-new-domain-awareness-surveillance-hq [https://perma.cc/5PTB-J7JA].

surreptitiously nabbing beverage cups from people they suspect, to asking for consent from victims or people they wish to clear in investigations and then retaining it.[23] San Francisco was embroiled in controversy after it became public that it was saving the DNA from sexual assault victims for later investigative use.[24]

This enormous data grab is happening today for little reason other than that technology has made it possible. As we walk about, living our lives, doing what we do, we can't help but reveal ourselves, and drop digital breadcrumbs.[25] Law enforcement now has the tools—cameras and sensors and such—that permit capturing this information, wholesale, from a distance.[26] The rapidly plummeting cost of storage has made it "technologically and financially feasible" for governments to "record nearly everything that is said or done within their borders—every phone conversation, electronic message, social media interaction, the movements of nearly every person and vehicle, and video from every street corner."[27] Finally, there's the use of artificial intelligence to pull all this information together into a remarkably complete picture of who you are, what you are doing, and what you might do next.[28]

Exemplary of where we are headed—and certainly head-turning—is the Department of Homeland Security's Fast Attribute Screening Technology (FAST), a set of "behavior-based screening

---

[23] *See* Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1492 (2015) (discussing the "growing number of unregulated local [DNA] databases"); Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 860–62 (2006) (describing techniques by which police have gathered or tricked suspects into providing DNA).

[24] Gregory Yee, *San Francisco Police Used Rape Victims' DNA to Try to 'Incriminate' Them, D.A. Says*, L.A. TIMES (Feb. 15, 2022, 10:27 PM), https://www.latimes.com/california/story/2022-02-14/san-francisco-police-misused-rape-victims-dna-chesa-boudin-says [https://perma.cc/HZT4-S57V].

[25] *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008) ("We leave traces of ourselves continually, including our location, our communications contacts, our consumption choices—even our DNA.").

[26] *See* Gregory Brazeal, *Mass Seizure and Mass Search*, 22 U. PA. J. CONST. L. 1001, 1008 (2020) (describing "[t]he proliferation of digital sensors and digital records" that allow the government "to conduct digital surveillance on a mass scale").

[27] JOHN VILLASENOR, RECORDING EVERYTHING: DIGITAL STORAGE AS AN ENABLER OF AUTHORITARIAN GOVERNMENTS 1, 3 (2011).

[28] *See* Cameron F. Kerry, *Protecting Privacy in an AI-Driven World*, BROOKINGS (Feb. 10, 2020), https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world [https://perma.cc/5278-HCBT] ("As artificial intelligence evolves, it magnifies the ability to use personal information . . . by raising analysis of personal information to new levels of power and speed.").

techniques" to ferret out who is safe to fly and who is not.[29] Reading about it is the stuff of dystopian science fiction, except it's real. It's based on the "Theory of Malintent," i.e., that people seeking to cause harm "may act strangely, show mannerisms out of the norm, or experience extreme physiological reactions based on the extent, time, and consequences of the event."[30] FAST relies on non-contact sensors that measure (among other things) your heart rate and respiration, your gaze and pupil diameter, facial features, expressions, and body movements, and perhaps more, such as "pheromone[] detection."[31] DHS claims FAST demonstrated over seventy percent classification accuracy using only remote, non-contact sensors, and thereby "validated the concept of using technology to detect malintent."[32]

Where FAST is a futuristic technology, automated license plate readers (ALPRs) are ubiquitous. ALPRs are just what they sound like—cameras that record passing license plates. They are mounted on mobile police cars or stationary sites like telephone poles. They capture every license plate that goes by. ALPR technology compares those plates in real time to a "hot list," looking for matches, or "hits," with license plates sought by law enforcement.[33] Today they are used to locate everything from vehicles fleeing from serious offenses to such trivial matters as stopping people with outstanding warrants for failing to pay parking tickets or property taxes.[34]

As storage costs dropped, policing agencies decided they not only could compare license plate reads with hot lists—they also could squirrel away all the ALPR information for later use in criminal investigations.[35] That way, if a criminal investigation turned up a license

---

[29] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 2 (2008) [hereinafter FAST IMPACT ASSESSMENT].

[30] *Id.*

[31] *Id.* at 3–4.

[32] DHS Science and Technology Directorate, *Future Attribute Screening Technology*, U.S. DEP'T OF HOMELAND SEC. (Nov. 18, 2014), https://www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST.pdf [https://perma.cc/25AR-BA8Y].

[33] ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 2 (July 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/3QZE-RYTZ].

[34] AXON AI & POLICING TECH. ETHICS BD., SECOND REPORT OF THE AXON AI & POLICING TECHNOLOGY ETHICS BOARD: AUTOMATED LICENSE PLATE READERS 14 (2019), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf [https://perma.cc/7Q4D-56NQ].

[35] *See* AUDITOR OF THE STATE OF CAL., REPORT 2019–118: AUTOMATED LICENSE PLATE READERS 1 (2020), https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [https://

plate number or a particular car, a database of where vehicles had been, and when, could be searched to identify suspects' whereabouts.

Artificial intelligence has changed the ALPR game entirely. Once expensive to purchase ALPR units, AI now allows ordinary low-cost cameras to become license plate readers.[36] Combined with dropping storage costs and data sharing, law enforcement is developing an all-encompassing system of geo-located surveillance.[37] Police cars, with cameras front and rear, can suck in license plate reads from multiple lanes of traffic at a time.[38] Policing agencies also partner with private vendors to gather yet more license plate reads.[39] Nationally, the pool of license plate reads is skyrocketing way into the billions, and agencies have agreements to share this pool with one another.[40]

The result is that with little supervision or regulation, police now have at their disposal a huge database of information that permits geo-tracking of all of us who drive cars. The geo-located ALPR data then flows into larger data holdings, allowing police to compile digital dossiers on countless entirely innocent people. With large grants following 9/11, Congress facilitated the creation of state and regional fusion centers, whose function is, as one might guess, to fuse together all this data in ways that are useful to the police.[41] There's remarkably little transparency around fusion centers—many are entirely unregulated—but we know they collect and store a mass of data acquired

---

perma.cc/V3FK-CHMA] (discussing how law enforcement agencies use ALPRs to "archive . . . historical images").

[36] *See* AXON AI & POLICING TECH. ETHICS BD., *supra* note 34, at 15 (discussing how AI can turn normal videos, fed through a laptop, into license plate readers).

[37] *See* Ángel Díaz, *New York City Police Department Surveillance Technology*, BRENNAN CTR. FOR JUST. (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology [https://perma.cc/8XYD-NSF6] (outlining, among other things, NYPD's use of ALPRs to create a vast storage of data that can be used to analyze movements of individuals and cars in relationship to crimes).

[38] *See, e.g.*, *Axon Fleet 3 Has Arrived: Next Generation In-Car Video System with ALPR Now Shipping to Public Safety Agencies*, AXON (June 30, 2021), https://www.multivu.com/players/English/8829452-axon-fleet-3-video-system-alpr-shipping-public-safety-agencies [https://perma.cc/2M53-9PHL].

[39] *Id.*

[40] *See* Byron Tau, *License-Plate Scans Aid Crime-Solving but Spur Little Privacy Debate*, WALL ST. J. (Mar. 10, 2021, 12:23 PM), https://www.wsj.com/articles/license-plate-scans-aid-crime-solving-but-spur-little-privacy-debate-11615384816 [https://perma.cc/Y3UT-735Q] (noting rise in license plate scanners and expanding data pools).

[41] *See* STAFF OF S. COMM. ON THE PERMANENT SUBCOMM. ON INVESTIGATIONS, 112TH CONG., FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 1 (Comm. Print 2012) (discussing the federal government's support for fusion centers to share terrorism-related information among local and federal police agencies).

from private brokers and police, including from license plate readers.[42]

The ready availability of technologies like ALPRs is changing law enforcement in profound ways. Policing has, in effect, moved to a model of social control, using data not only to investigate those suspected of crime, but also to ensure all of us keep our noses clean.[43] No longer need policing agencies wait until a crime occurs, or even for a tip that one might. Predictive analytics are used to direct them to where crime is anticipated to occur, or to people who are believed to be prone to criminal activity.[44] One satisfied police chief in the tiny, affluent village of Sands Point on Long Island bragged that "[w]e have every access point to our village covered. . . . It makes it a gated community without putting a gate up."[45] If you think about it, that's not so different than what we do with No Fly Lists, or gang databases, which, when paired with facial recognition on private cameras at shopping malls, may limit the ingress of "undesired" customers.[46] To be sure, we are not China, or Myanmar. But we uncontestably have the capacity to be, and in some instances we are edging powerfully close.[47]

---

[42] *See* Danielle K. Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1451 (2011) (outlining the vast amount of data stored by fusion centers).

[43] *See* Balkin, *supra* note 25, at 12 (discussing how state surveillance often is used to signal to people that they are being watched and should behave); Friedman & Ponomarenko, *supra* note 14, at 1884 (discussing deterrent-based policing strategies like drunk-driving checkpoints that "use the threat of detection to keep people within the lines of the law"). Particularly for minority populations, policing has always been at times a tool of social control, *see* Sandra Bass, *Policing Space, Policing Race: Social Control Imperatives and Police Discretionary Decisions*, 28 SOC. JUST. 156 (2001) (discussing the relationship between race and policing), but the technological means to accomplish this on a widespread basis are changing the nature of policing today.

[44] *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT chs. 3–4 (2017) (discussing police use of predictive technologies); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 55–56 (2014) (discussing how police are using "predictive policing software to direct them to places where they believe there is a high likelihood of criminal activity"); Balkin, *supra* note 25, at 10 (discussing how the increasing use of surveillance supplements a policing "model of prosecution and deterrence with technologies of prediction and prevention").

[45] Tom Simonite, *AI License Plate Readers Are Cheaper—So Drive Carefully*, WIRED (Jan. 27, 2020, 8:00 AM), https://www.wired.com/story/ai-license-plate-readers-cheaper-drive-carefully [https://perma.cc/RE2K-RLM5].

[46] *See* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1790 (2016) (discussing the use of "identity determinations" that when combined with "No Fly List[s]" can be used to restrict the ability of individuals to engage in certain types of behavior, rights, or activities).

[47] *See, e.g.*, *Factsheet: The NYPD Muslim Surveillance Program*, ACLU, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program [https://perma.cc/94CF-S2BV] (discussing the all-encompassing, "suspicionless" surveillance program that the NYPD engaged in and aimed at Muslim communities after 9/11); Alvaro M. Bedoya, *The*

B. The Harms of Totalizing Surveillance

As I will explain shortly, some of this surveillance may serve beneficial purposes. Unregulated, though, it also has the capacity to impose great harm. Others already have documented the harms inherent in this sort of totalizing surveillance at length, so I will be brief.[48]

First, there are the innumerable errors that occur, many of them difficult to avoid with surveillance occurring at the scale we are experiencing, and yet each potentially devastating to the people involved.[49] Albert Florence was picked up for an outstanding warrant on a fine that had been paid but was erroneously recorded as open. He spent seven days in jail and was strip-searched twice in that time.[50] Robert Julian-Borchak Williams suffered a similar false arrest, this time because a facial recognition algorithm wrongly identified him for shoplifting from a high-end boutique. Despite his denying the image was him ("You think all black men look alike?") he spent thirty hours in jail, and his wife had to claim an "emergency" to his employer lest he risk losing his job.[51] Oakland police held on the ground, at gunpoint, a person wrongly identified by a license plate reader as driving

---

Color of Surveillance, SLATE (Jan. 18, 2016, 5:55 AM), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html [https://perma.cc/YW9S-WAQ5] (discussing use of surveillance against Black Lives Matter activists); NIKKI JONES, THE CHOSEN ONES: BLACK MEN AND THE POLITICS OF REDEMPTION (2018) (describing Black residents leaving communities to avoid surveillance of their bodies).

[48] *See generally* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002) (arguing that surveillance deprives us of our right to anonymity); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1101–04 (2002) (outlining the many harms of surveillance from law enforcement, from the abuse of personal information databases to using data to target disfavored groups or individuals); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (explaining how surveillance chills the exercise of civil liberties and increases the risk of discrimination, coercion, and selective prosecution).

[49] *See, e.g.*, Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations [https://perma.cc/8YD6-46PQ] (discussing the prevalence of ALPR inaccuracies, which lead to erroneous arrests).

[50] Robert Barnes, *Supreme Court Is Asked About Jails' Blanket Strip-Search Policies*, WASH. POST (Sept. 12, 2011), https://www.washingtonpost.com/politics/supreme-court-is-asked-about-jails-blanket-strip-search-policies/2011/09/09/gIQAuc6vNK_story.html [https://perma.cc/M4VZ-VQTN].

[51] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/QQM9-FMSF].

a stolen car. Their bad luck was that it was the Chair of Oakland's Privacy Commission.[52]

Then there's ugly misbehavior by our watchers. It's apparently difficult to resist dipping into all this stored data at times, the most characteristic misuse of which seems to be peeping into the lives of romantic interests.[53] A legislative audit found that *over half* of the 11,000 law enforcement personnel who searched the Minnesota Department of Public Safety driver database conducted searches that were "questionable."[54]

But the aggregate greater harms aren't because of mistakes and misbehavior—they occur when the systems work precisely as they are intended. Often this harm is referred to as threatening "privacy," but as many have observed, the real threat here is to people's sense of "security"—the very word that is used in the Fourth Amendment.[55] In *Riley v. California*, involving the search of a cell phone incident to a lawful arrest, the Chief Justice described what can be gleaned from nothing other than pictures on our cell phones: "The sum of an individual's private life can be reconstructed [from] a thousand photographs labeled with dates, locations, and descriptions."[56]

Of course, this surveillance does not affect everyone equally; like too much in the United States, it is raced and classed.[57] When the

---

[52] Nate Gartrell & David Debolt, *"They Went Cowboy on Us": Privacy Advocate Says East Bay Police Held Him at Gunpoint over License Plate Reader Mix-Up*, MERCURY NEWS (Feb. 17, 2019, 4:10 PM), https://www.mercurynews.com/2019/02/15/they-went-cowboy-on-us-privacy-advocate-says-police-held-him-at-gunpoint-over-license-plate-reader-mishap [https://perma.cc/W6EE-2TRJ].

[53] *See, e.g.*, Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, AP NEWS (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43 [https://perma.cc/FNH5-DBRJ] (describing officers' frequent checking on romantic partners using databases); Siobhan Gorman, *NSA Officers Spy on Love Interests*, WALL ST. J. (Aug. 23, 2013), https://www.wsj.com/articles/BL-WB-40005 [https://perma.cc/9YSS-GF5W] (describing how the practice of NSA officers spying on romantic partners was so common it garnered its own "spycraft label: LOVEINT").

[54] STATE OF MINN. OFF. OF THE LEGIS. AUDITOR, LAW ENFORCEMENT'S USE OF STATE DATABASES 26 (2013), https://www.auditor.leg.state.mn.us/ped/pedrep/ledatabase.pdf [https://perma.cc/WLH2-NWVB].

[55] *See, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008) (arguing that Fourth Amendment caselaw should refocus on guaranteeing a right to security over a right to privacy). *See generally* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1050 n.33 (2016) (citing a wealth of sources urging focus on "security").

[56] Riley v. California, 573 U.S. 373, 394 (2014).

[57] *See* BARTON GELLMAN & SAM ADLER-BELL, THE CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE (2017), https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf [https://perma.cc/RX6U-H9TD] (analyzing the disproportionate impact of mass surveillance on communities identified by poverty, race, religion, and immigration status); *see also Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/

government determines to collect and use information against people, there's a good chance those who suffer most will be Black and brown.[58] That the ill effects of pervasive surveillance fall on the less well-off and less white is a feature, not a bug.[59] As Danielle Citron says, in her review of Khiara Bridges's book, *The Poverty of Privacy Rights*, "[w]hen it comes to poor mothers specifically, the State's data collection efforts are boundless and inescapable."[60]

Even focusing on the specific security and privacy interests of individuals, though, may underplay what's more fundamentally at stake, which is that placing dossiers on everyone in government hands is insidious to liberty itself. In a recent report, the Federation of American Scientists interviewed many stakeholders about the concerns with the proliferation of data collection technologies in use by governments.[61] Respondent after respondent highlighted the "very serious threat to the future of democracy, human rights, and the rule of law around the world."[62] As current events around the globe make clear, the danger is hardly hypothetical.

---

pages/automated-license-plate-readers-alpr [https://perma.cc/2P4J-2USB] (reporting how ALPR technology is deployed discriminatorily to target Muslim communities). *See generally* David H. Gans, "*We Do Not Want to be Hunted": The Right to be Secure and Our Constitutional Story of Race and Policing*, 11 COLUM. J. RACE & L. 239 (2021) (discussing how police power historically has been used in discriminatory ways against Black Americans).

[58] *See, e.g.*, Vincent M. Southerland, *The Intersection of Race and Algorithmic Tools in the Criminal Legal System*, 80 MD. L. REV. 487, 498 (2021) (describing the tendency of algorithmic tools used in policing to be racially biased); Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301, 306 (2020) (explaining surveillance often is used as "a tool to stop marginalized people from achieving power"); Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 144 (2021) ("[B]ecause the underlying data encodes existing racial inequity in policing, predictive policing may learn and replicate bias."); 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, 18 (2019) (discussing how "dirty data" infects algorithmic systems leading to racial bias); Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/5LRB-8W66] (concluding that increased use of facial recognition software by police "will disproportionately affect African Americans").

[59] *See* Amna Toor, *"Our Identity is Often What's Triggering Surveillance": How Government Surveillance of #BlackLivesMatter Violates the First Amendment Freedom of Association*, 44 RUTGERS COMPUT. & TECH. J. 286, 294–301 (2018) (tracing the long history of government surveillance of Black communities).

[60] Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1142 (2018) (reviewing KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017)).

[61] *See* ISHAN SHARMA, FED'N OF AMERICAN SCIENTISTS, A MORE RESPONSIBLE DIGITAL SURVEILLANCE FUTURE 6–7 (2021), https://fas.org/wp-content/uploads/2021/02/Digital-Surveillance-Future.pdf [https://perma.cc/G7JC-J5XH].

[62] *Id.* at 7.

Nor does the "it can't happen here" argument get one very far because it could, and it has. Edward Snowden tipped us all off to the massive data grab on all of us following 9/11.[63] Even if the watchers initially had pure motives, what matters is how the data eventually is used. The Red Scares gathered up many hapless individuals based on data surveillance.[64] The internment of the Japanese Americans was facilitated by data surveillance.[65] For decades, as part of its COINTELPRO operation, the United States intelligence community not only kept tabs on the Civil Rights and Women's Rights movements, but also all too often attempted to intervene in ways that were, yes, insidious to democracy.[66] The federally supported state and regional "fusion center" intelligence-gathering hubs repeatedly have been caught spying on entirely lawful First Amendment activity, including labeling legitimate candidates for office and Catholic nuns as security threats and tracking environmental activists and the Black Lives Matter movement.[67]

To be clear—and clarity is important here because I am not arguing all this technology necessarily is a bad thing—the kind of surveillance described here often is conducted for the purest of motives, and there is some evidence that it can make us safer. Policing agencies have engaged in full-throated adoption of these technologies for the same reason most of us did: There was a new tool that promised to let us do whatever it is we do, better. The government used facial recognition and a variety of databases to identify the January 6, 2021 insurrectionists.[68] DNA collected from arrestees and others has helped

---

[63] *See Edward Snowden Discloses U.S. Government Operations*, HISTORY.COM (June 26, 2018), https://www.history.com/this-day-in-history/edward-snowden-discloses-u-s-government-operations [https://perma.cc/UBR3-VYHK] (explaining how the Snowden leaks exposed an NSA program that collected communication records of Americans).

[64] *See* Solove, *supra* note 48, at 1110–11.

[65] *Id.* at 1110; *see also* William Seltzer & Margo Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses*, 68 SOC. RSCH. 481, 484 (2001) (noting use of surveillance data in instances of human rights abuses including the Nazi Holocaust, internment of Japanese Americans, forced removal of Native Americans, forced migration of minority populations in the USSR, and the Rwandan genocide).

[66] *See* Toor, *supra* note 59, at 295–98 (discussing how the FBI surveilled civil rights groups and sought to discredit leaders and disrupt recruitment efforts).

[67] *See* Will Parrish & Jason Wilson, *Revealed: Anti-Terror Center Helped Police Track Environmental Activists*, THE GUARDIAN (Oct. 2, 2019), https://www.theguardian.com/us-news/2019/oct/02/oregon-pipelines-protests-monitoring-police-anti-terror-unit [https://perma.cc/KWN8-BZ5A] (describing how Oregon Titan Fusion Center monitored groups protesting a fossil fuel project in the state and supporters of the Black Lives Matter movement); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 81 (2013) (discussing how in one instance Maryland state police labelled fifty-three political activists terrorists based on their access to fusion centers).

[68] *See* Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM), https://

solve cold cases.[69] Agencies like the SEC mine data to find those committing fraud on the market.[70]

There are two problems, however. First, the actual value of this sort of surveillance rarely is assessed.[71] In the giant ongoing data grab, no one pauses to figure out whether any particular collection and use of data—like the billions of license plate reads—is worth the costs and risks. Some may be, some not. Second, and closely related, there's absolutely no regulation of most of this. The impetus of regulation might cause us to be more thoughtful, overall, about the value and threat of what we are doing. It might cause us to use our technological capabilities wisely, when it is most beneficial. And it might spur adoption of safeguards that are all too absent today.

C. The Utter Haplessness of Fourth Amendment Doctrine

One might think, naively, that the Fourth Amendment would offer some protection.[72] After all, the Justices tell us that "a central aim of the Framers was 'to place obstacles in the way of a too-permeating police surveillance.'"[73] And in recent cases involving "innovations in surveillance tools," the Court has taken to insisting the Amendment "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was

---

www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy [https://perma.cc/6SPV-TVV3].

[69] *See* What Next: TBD, *What Cops Are Doing with Your DNA*, SLATE (June 18, 2021, 6:00 AM), https://slate.com/podcasts/what-next-tbd/2021/06/do-you-still-own-your-dna [https://perma.cc/9FK8-MS48] (discussing law enforcement's use of genetic genealogy technology and open-source DNA platforms to apprehend the Golden State Killer).

[70] *See* Rachel E. Barkow, *The New Policing of Business Crime*, 37 SEATTLE U. L. REV. 435, 439 (2014) (discussing the use of datamining in SEC enforcement); Charles S. Clark, *IRS and SEC Detect Fraud Patterns in Heaps of Data*, GOV'T EXEC. (Oct. 16, 2012), https://www.govexec.com/technology/2012/10/irs-and-sec-detect-fraud-patterns-heaps-data/58816 [https://perma.cc/WH48-Z4J3] (describing how the IRS and SEC utilize data mining tools and social media to detect fraud).

[71] CCTV presents an all-too-rare example of trying to assess the value of surveillance empirically. *See, e.g.*, Sonia Roubini, *Police Chief: Surveillance Cameras Don't Help Fight Crime*, ACLU (Apr. 9, 2015, 3:00 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-chief-surveillance-cameras-dont-help-fight [https://perma.cc/7SL4-SKY6] (explaining how government authorities that use surveillance technology rarely monitor and audit its performance); Noam Biale, *Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found*, ACLU (2008), https://www.aclu.org/sites/default/files/images/asset_upload_file708_35775.pdf [https://perma.cc/5GAK-HY8X] (finding strong indications that video surveillance has little to no positive impact on crime).

[72] *Accord* Balkin, *supra* note 25, at 19 ("You might think the Fourth Amendment would be the most important constitutional provision for controlling and preventing abuses of power in the National Surveillance State.").

[73] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citing United States v. Di Re, 332 U.S. 581, 585 (1948)).

adopted."[74] The one thing about the origins of the Fourth Amendment on which everyone agrees is that it was aimed at "general warrants," which is to say government indiscriminately intruding and collecting information on the public without regard to whether there was suspicion—reasonable or otherwise—that any given person had done anything wrong.[75] That seems to many to be precisely what is going on here.[76]

In reality, however, the Supreme Court's doctrine does little to regulate digital surveillance, and even less for surveillance in bulk. The problem rests with how the Justices define what a "search" within the meaning of the Fourth Amendment is.[77] According to the Court, whenever we act in public, we have "voluntarily conveyed" information to the world, and hence the police.[78] Where we drive our cars, whether we visit a therapist, quietly attend a substance use support group, or drop in on a lover, all that seems to be fair game. And under the "third-party doctrine," whatever we hand over to a third party, even in confidence or intending it to be private, nonetheless can be obtained by the police without even a warrant.[79] Not only the private papers you give to your accountant, but every digital breadcrumb you leave on the internet or in an app, be it your location, your use of a credit card or a phone, or much else.[80]

---

[74] *Id.* at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

[75] *See* Gans, *supra* note 57, at 258 ("[T]he driving impetus for inclusion of the Amendment was the fear that the federal government might reinstitute general warrants . . . ."); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 366 (1974) ("[T]he primary abuse thought to characterize the general warrants . . . was their indiscriminate quality, the license that they gave to search Everyman without particularized cause.").

[76] *See* Gray & Citron, *supra* note 67, at 99 ("The concerns about broad programs of indiscriminate search that drove us to adopt the Fourth Amendment in 1791 are raised anew with law enforcement's unfettered access to contemporary surveillance technologies.").

[77] *See* Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 568 (2017) ("For the Fourth Amendment to apply, government agents must conduct a 'search' or a 'seizure.'").

[78] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("A person travelling in an automobile . . . voluntarily conveyed to anyone who wanted to look . . . the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.").

[79] *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . .").

[80] *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 268 (2016) ("Almost every aspect of online life now leaves a trail of digital breadcrumbs in the form of third-party records. Every phone call, every email, every search and click online can create a third-party record.").

The Justices' laissez-faire attitude toward police spying has generated a flood of critical commentary, which seems to have altered their course not at all. There are frequent calls to overturn the third-party doctrine or tighten up the definition of what constitutes a search.[81] Theories abound about how to reinterpret the Constitution—particularly the Fourth Amendment—to make it serviceable in regulating data surveillance.[82]

Some more recent cases pull back a bit from the brink, revealing that the Justices themselves are concerned about the surveillance problem but are uncertain what to do about it. In 2012, in *United States v. Jones*, the Supreme Court held that GPS tracking of a vehicle constituted a search. The majority opinion rested on a physical trespass theory: The police had physically attached a beeper to the car to gain information.[83] But as the concurring Justices in Jones pointed out, a trespass approach will prove slim protection in a world in which most surveillance requires no physical intrusion.[84] The five Justices who concurred in *Jones* demonstrated a keen awareness of the dangers of invasive surveillance.[85] Still, all they could offer up in response

---

[81] *See, e.g.*, Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1401–03 (2008) (calling for an end to the third-party doctrine); DANIEL J. SOLOVE, THE DIGITAL PERSON 220–21 (Jack M. Balkin & Beth Simone Noveck eds., 2004) (proposing that police be required to show probable cause before accessing third-party data held in a "system of records"); Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Spaces*, 63 AM. U. L. REV. 21, 48 (2013) (proposing "to treat all police recording of public movements and activities that occur outside the presence of the officer doing the recording as a Fourth Amendment search"); Gray & Citron, *supra* note 67, at 71–72 ("[T]he threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy . . . .").

[82] *See, e.g.*, Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 999 n.236 (2016) (adopting a property based approach to determining which effects are protected by the Fourth Amendment, and suggesting that approach might work for digital data); Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 309–10 (2011) (suggesting revising the doctrine to deal with dragnet searches, including digital ones, by restoring a warrant requirement, but also by disfavoring dragnets if an individualized-suspicion search would meet government needs); Brazeal, *supra* note 26, at 1004 (advocating for a "programmatic review of digital mass surveillance programs" utilizing Fourth Amendment seizure, not search, doctrine).

[83] *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

[84] *See id.* at 414 (Sotomayor, J., concurring) ("[P]hysical intrusion is now unnecessary to many forms of surveillance."); *id.* at 426 (Alito, J., concurring) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact . . . .").

[85] *See id.* at 428 (Alito, J., concurring) ("Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements."); *id.* at 416 (Sotomayor, J., concurring) ("GPS monitoring . . . may 'alter the relationship between

was that although warrantless short-term GPS tracking was constitutional, an unspecified amount of long-term tracking was not.[86]

Concurring in *Jones*, Justice Alito made the point that technology simply had the Court outgunned. Back in the day, if the police wanted to keep tabs on someone's whereabouts 24/7 for an extended period, they'd need a fleet of super stealthy detectives operating in shifts. Even then, it wasn't easy. Only the most serious of cases remotely would justify the expense.[87] Today, it's a quick application to Verizon or Sprint and a small fee to do the same. And while technological developments continue at a meteoric pace, the Justices engage in an eighteenth-century version of common-law decisionmaking in which they manage at most to offer up some pronouncement of importance once every few years. This is no way to get burgeoning police use of technology under control.

Justice Alito's solution is that legislative bodies need to step in and regulate surveillance technology, but wishing this will happen is different than making it so.[88] Legislative bodies have been reluctant to act, for obvious reasons. What precisely is in it for any given legislator,

---

citizen and government in a way that is inimical to democratic society.'" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011))).

[86] *See id.* at 430 (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

[87] *See id.* at 429 ("Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources.").

[88] *Id.* at 429 ("[T]he best solution to privacy concerns may be legislative."). Many commentators have urged a legislative or administrative solution to fill the constitutional vacuum. *See* Primus, *supra* note 82, at 309–10 (suggesting requiring "a statute that clearly defines when and how the government should perform an administrative intrusion with sufficient limitations on government discretion"). *See, e.g.*, Mariano-Florentine Cuéllar & Aziz Z. Huq, *Economics of Surveillance*, 133 HARV. L. REV. 1280, 1334–35 (2020) (arguing for new regulatory frameworks); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1187 (2017) (reviewing FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015)) (same); Mailyn Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 SANTA CLARA HIGH TECH. L.J. 481, 481 (2020) (advocating for "local administrative governance by city councils or local administrative agencies"); Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 FORDHAM L. REV. 779, 782–83 (2005) (proposing legislative rule-creation by Congress to regulate developing surveillance technologies); Renan, *supra* note 55, at 1075 (suggesting framework legislation of administrative law as "a mechanism independent from constitutional criminal procedure to govern surveillance"); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 328 (2008) ("Legislation is ultimately the best means of regulating data mining, given its complexity."); Friedman & Ponomarenko, *supra* note 14, at 1832 (arguing for increased legislative involvement in policing); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 134 (2016) (arguing that the Administrative Procedure Act and administrative law should provide a framework for regulating police behavior).

let alone a majority of them, to tie the hands of policing agencies? Many commentators have documented the powerful public choice forces that keep legislators from stepping up in this space, be they the fear of being attacked as soft on crime or concern about the power of police and prosecution lobbies.[89] To be sure, occasionally some sort of surveillance becomes so salient that a legislative body acts—as the U.S. Congress did in the USA FREEDOM Act responding to Edward Snowden's revelations.[90] But that was years after most people in Congress knew, and still it took a public ruckus of rare dimensions to motivate Congress to address the problem.[91]

Many have read the Supreme Court's 2018 decision in *Carpenter v. United States* as a watershed, but there's every reason to be skeptical that *Carpenter* will rescue us from the sort of overweening surveillance at issue here. That case invalidated a police request for seven days of cell site location information of one mobile phone user who was suspected of being involved in a number of robberies, deeming it a "search" that required a warrant.[92] Still, the majority characterized its opinion as "narrow" and once again offered up no clearly identifiable test.[93] It simply claimed it was declining to "extend" the third-party doctrine to this new form of information gathering.[94] The Court was sharply divided, with Ruth Bader Ginsburg providing a necessary fifth vote. It is unclear if Amy Coney Barrett, who replaced Justice

---

[89] *See generally* Barry Friedman & Elizabeth G. Jánszky, *Policing's Information Problem*, 99 TEX. L. REV. 1, 24–45 (2020) (offering public choice theory as an explanation for legislative inaction around policing); Rachel E. Barkow, *Federalism and the Politics of Sentencing*, 105 COLUM. L. REV. 1276, 1278–83 (2005) (describing how tough-on-crime politics contributes to severity in sentencing); William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 530 (2001) (explaining how politicians are incentivized to pander to voters by passing mandatory minimum sentences and "three strikes" laws).

[90] *See* Bart Forsyth, *Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection*, 72 WASH. & LEE L. REV. 1307, 1308–09 (2015) (explaining how Snowden's leaks were the impetus for the USA FREEDOM Act).

[91] *See* Alisa Chang, *What Did Congress Really Know About NSA Tracking?*, NPR: IT'S ALL POLITICS (June 11, 2013, 5:26 PM), https://www.npr.org/sections/itsallpolitics/2013/06/11/190742087/what-did-congress-really-know-about-nsa-tracking [https://perma.cc/N838-KYWK] (reporting that members of Congress had been briefed on NSA surveillance programs as early as 2009); Forsyth, *supra* note 90, at 1321–24 (characterizing the passage of the USA FREEDOM Act as slow and labored despite broad congressional support).

[92] Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018). Even that was curious, because the police only had received two days' worth in response. *Id.* at 2226 (Kennedy, J., dissenting).

[93] *Id.* at 2220 (majority opinion); *see* Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1805 (2022) ("The Supreme Court [in *Carpenter*] gave no concrete test to guide future decisions . . . .").

[94] *Carpenter*, 138 S. Ct. at 2220.

Ginsburg, will similarly be inclined to reel in government surveillance. Even if she does, one might guess she will be attracted to Justice Gorsuch's advocacy for a more positive-law approach, leaving the law yet more fractured and uncertain.[95] Lower courts have relied on *Carpenter* to strike some particularly invasive tactics, but the use has been spotty at best.[96] Most significantly, *Carpenter* dealt with surveillance of an individual, not the mass digital surveillance that concerns us here.[97]

What's worthy of our attention is *why* the Court is struggling to rein in sprawling surveillance, because those reasons are likely to define what a workable solution might look like. First, the Justices are every bit in the dark as the rest of us as to the efficacy of these surveillance practices. The dissenting Justices in *Carpenter* played Chicken Little ("the sky is falling!") at the notion the government could not simply subpoena any information it wanted that rested in third-party hands.[98] But the truth is neither they nor anyone else has offered up systematic evidence of the efficacy of the exploding surveillance we are experiencing. Second, if anything, the Court as a whole is biased in favor of thinking surreptitious government information collection works, because most of what they know is from cases seeking to suppress evidence that such surveillance revealed. They are utterly ignorant of the vast majority of cases in which such surveillance posed all the risks detailed above, but revealed absolutely nothing.[99] Third, there's a structural bias atop the factual one—given the nature of judicial review, if the Justices rule something unconstitutional, that is beyond a legislative fix. Judicial review effectively makes the Justices' decision all-or-nothing. For this reason, they understandably are tentative in saying no to the police given that, for all they know, the surveillance efforts of policing agencies are valuable in keeping us safe.[100] Finally, there is the seeming lack of tools at their disposal. Warrants based on probable cause are not of much value when mass data collec-

---

[95] *See id.* at 2268 (Gorsuch, J., dissenting) (advocating for "[a] Fourth Amendment model based on positive legal rights").

[96] *See generally* Tokson, *supra* note 93, at 14–26 (examining all 857 state and federal judgments that have cited *Carpenter* since its publication).

[97] A rare example of *Carpenter* being used to invalidate mass surveillance was *Leaders of a Beautiful Struggle v. Baltimore Police Department*, in which the divided en banc United States Court of Appeals for the Fourth Circuit struck down Baltimore's use of aerial surveillance. *See* 2 F.4th 330 (4th Cir. 2021) (en banc).

[98] *See infra* note 311.

[99] FRIEDMAN, *supra* note 14, at 82–83 (discussing bias in that judges only see what is presented in the case before them).

[100] *See Carpenter*, 138 S. Ct. at 2220 ("[T]he Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'" (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944))).

tion is at issue. It's no accident that the cases the Justices have considered tend to be around surveillance targeted at individuals, and their own doctrines deny standing to most people to challenge surveillance *en masse*.[101] On the topic of this paper, they have stood mute.

Virtually every commentator in the space has concluded that the Fourth Amendment is hapless when it comes to digital surveillance.[102] And as we've seen, legislative bodies aren't much help either. Ben Wittes puts it aptly: "Most of this data is not plausibly protected by the Fourth Amendment. Much of it is not protected by any law at all."[103] We live in an age of lawless surveillance, and when it comes to doing something about it, we're getting nowhere fast.

II
The Constitutional Law of Personal Data Collection

Fortunately, there is an alternative means of motivating change, one that addresses many of the problems the Justices face in getting surveillance under control. It is an alternative that does not require the Justices to understand or even care about the efficacy of the surveillance tools, does not leave them susceptible to decisional bias based on the conduct of a specific defendant (or the government for that matter), and most significantly does not necessitate their ruling any particular police surveillance data collection technique off the table entirely as a matter of constitutional law. Rather, it simply requires them to say: "Before you (policing agency) do this, you must have appropriate legislative authorization, and a basic regulatory scheme in place." At present, the default is that policing agencies do as they wish, until they are stopped by legislative action.[104] Under the Constitution, properly understood, this default is flipped on its head.

---

[101] *See* ACLU v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015) (finding that standing to challenge the government's cellphone metadata collection program requires that "appellants have suffered a concrete and particularized injury fairly traceable to the challenged program and redressable by a favorable ruling").

[102] *See, e.g.*, Balkin, *supra* note 25, at 19 ("[C]ourts have largely debilitated the Fourth Amendment to meet the demands of the Regulatory and Welfare States, the National Security State, and the War on Drugs."); Brazeal, *supra* note 26, at 1003 ("[T]he Fourth Amendment . . . currently provides no protection against the vast majority of existing and possible forms of digital mass surveillance.").

[103] Benjamin Wittes, Brookings Inst., Databuse: Digital Privacy and the Mosaic 12 (2011).

[104] *See* Meghan Holloway, *Penalty Default Rules for Digital Searches: Why Courts Should Spur Legislative Action via Second-Order Regulation*, 87 U. Chi. L. Rev. 1395, 1425 (2020) ("Because . . . digital search default rules do not interfere with the status quo, police departments feel no need to lobby policymakers to pass laws to change them. Policymakers thus are not motivated to replace the default rules with alternatives.").

The Supreme Court—all courts—should hold that government surveillance data collection may not move forward unless and until there is a regulatory scaffolding undergirding it.

The purpose of this Part is to show that in numerous areas in which the government seeks our personal data, courts require just that: a regulatory scheme comprised of a common set of constitutional prerequisites. Specifically, prior to obtaining personal information about us, there must be: democratically accountable authorization; a clear justification or reason for the surveillance; a program designed to achieve that regulatory purpose; regularity of collection (i.e., not left to officer arbitrariness); safeguards to protect individual concerns, such as minimizing the collection of unnecessary information; and the opportunity for judicial review. In case after case, under one constitutional clause after another, courts—particularly the Supreme Court—expect this of government in advance of collecting personal information. Although many of the cases and contexts of information collection in the discussion that follows differ both from one another, and from police surveillance, what matters is what unites them. Each example, no matter the context, involves the government's acquisition of personal information. And in each instance, courts require the same sort of regulatory prerequisites before the collection occurs.

A. The Fourth Amendment and Subpoenas

We are going to begin our constitutional tour—and as it happens end it—with the Fourth Amendment, albeit in contexts outside of digital surveillance. There is a reason. Both with subpoenas (where we begin), and "special needs" searches (where we conclude), courts find the government's conduct to be a "search" governed by the Fourth Amendment but require neither warrants nor probable cause.[105] Rather, government information collection simply requires regulatory prerequisites in place before collection occurs. That is precisely what should happen around police surveillance.

From the nation's founding, government has been authorized, as it was in Great Britain, to use subpoenas to compel subjects to produce information.[106] And throughout this country's history, this authority has been challenged—as the cases I am about to discuss make clear—on the ground that subpoenas are Fourth Amendment

[105] I have split up these differing Fourth Amendment approaches to government data collection because this Part moves from collection of individual data to more programmatic collection, which is what "special needs" searches are.

[106] *See generally* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 810–26 (2005) (providing background on the history of the subpoena from Great Britain to America).

"searches" or "seizures" that both are "unreasonable" and require warrants based on probable cause. These arguments enjoyed a brief moment of success before collapsing in the face of the government's insatiable need for "the fuel without which the administrative engine could not operate."[107] Even in collapse, though, courts required a regulatory structure that, if applied to mass data surveillance, would change the rules of the game entirely.

The story begins with *Boyd v. United States*, in which the government introduced into evidence invoices it had subpoenaed in the course of a forfeiture against thirty-five cases of plate glass claimed to have been imported without the necessary duty having been paid.[108] The question in *Boyd* was whether "compulsory production of a man's private papers . . . to be used in evidence against him" is an "'*unreasonable* search and seizure' within the meaning of the [F]ourth [A]mendment of the Constitution[.]"[109] The Court concluded yes: "[P]apers are the owner's . . . dearest property, and are so far from enduring a seizure, that they will hardly bear an inspection . . . ."[110] One might protest that no search occurred in *Boyd* at all; no one broke into a home or office to grab papers, they merely were subpoenaed. But for the *Boyd* majority, this missed the entire point: "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . ."[111]

Confronting the necessities of the administrative state, in which information is essential to regulation, the Supreme Court ultimately brushed *Boyd* aside, holding that while subpoenas were indeed "searches and seizures," no warrant nor probable cause was necessary to their issuance.[112] Rather, as the Court explained in the 1906 case of *Hale v. Henkel*, the "search" by subpoena need only be "reasonable"—consistent with the Fourth Amendment's ban on "unreasonable searches and seizures."[113] "[T]he search and seizure clause of the [Fourth] Amendment was not intended to interfere with the power of courts to compel, through a *subpoena duces tecum*, the production, upon a trial in court, of documentary evidence."[114]

---

[107] Steve R. Johnson, *Reasonable Relation Reassessed: The Examination of Private Documents by Federal Regulatory Agencies*, 56 N.Y.U. L. REV. 742, 749 n.45 (1981).

[108] Boyd v. United States, 116 U.S. 616 (1886).

[109] *Id.* at 622.

[110] *Id.* at 627–28.

[111] *Id.* at 630.

[112] *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208–09 (1946).

[113] Hale v. Henkel, 201 U.S. 43, 73, 76 (1906).

[114] *Id.*

In *Oklahoma Press Publishing Co. v. Walling*, in 1946, the Supreme Court then identified the prerequisite elements of reasonableness to be applied to determine whether the "search" by subpoena was constitutional. These prerequisites apply to this day.

The first prerequisite is that there must be statutory authorization before government collects private information.[115] As we will see, it is difficult to find any case that allows government information collection without statutory authorization. In *Oklahoma Press*, the challenge was to the enforcement of a subpoena by the Wage and Hour Administrator under the Fair Labor Standards Act. The Court reviewed the relevant statute and found there was sufficient authorization: "The section thus authorizes both general and specific investigations, one for gathering statistical information concerning entire industries, . . . [and] the other to discover specific violations."[116]

The information sought also has to be relevant to a legitimate purpose; fishing expeditions are not permitted.[117] The government cannot simply pull in huge amounts of information without some basis for suspecting criminality. The *Hale v. Henkel* Court disallowed enforcement of a subpoena on just this ground.[118] Justice Holmes was at his indignant best in *FTC v. American Tobacco Co.*: "It is contrary to the first principles of justice to allow a search through all the respondent's records, relevant or irrelevant, in the hope that something will turn up."[119] The *Oklahoma Press* Court reiterated (citing *American Tobacco*), that no subpoena could "call[] for documents so broadly or indefinitely that it was thought to approach . . . the character of a general warrant."[120]

Although the required nexus between the specific information demanded and a legitimate ongoing investigation can be quite lenient, the limitation is a real one. When, for example, the Resolution Trust Corporation attempted to subpoena information on the net worth of officers and directors of failed Savings and Loans, courts balked.[121] As the Circuit Court for the District of Columbia put it:

---

115 *See Okla. Press*, 327 U.S. at 209.

116 *Id.* at 199 n.23.

117 *See id.* at 209; FTC v. Am. Tobacco Co., 264 U.S. 298, 305–06 (1924) (stating that anyone who respects the Fourth Amendment would be "loath" to believe that Congress intended the FTC "to direct fishing expeditions into private papers on the possibility that they may disclose evidence of crime").

118 *See Hale*, 201 U.S. at 76–77 (invalidating a subpoena as unreasonable because it was too sweeping and unnecessary to any potential criminal prosecution).

119 *Am. Tobacco Co.*, 264 U.S. at 306.

120 *Okla. Press*, 327 U.S. at 207.

121 *See* Resol. Tr. Corp. v. Walde, 18 F.3d 943, 949 (D.C. Cir. 1994) (rejecting the claim that RTC could request wealth information from former bank directors without any assertion of possible liability); *see also* Fed. Deposit Ins. Corp. v. Garner, 126 F.3d 1138,

> Much as we strain our imagination, we cannot find any way in which alimony payments or irrevocable trusts that predate appellants' association with a failed S&L and to which no assets may be transferred are relevant to whether appellants might be guilty of fraud, negligence, or breach of fiduciary duties.[122]

Indeed, the Fourth Amendment's "reasonableness" requirement imposes an even higher showing when the government seeks particularly personal information. In a relentless quest to locate wealth drained from failed savings and loans, the Reconstruction Trust Company sought personal financial information from former officers. But the D.C. Circuit demurred:

> Because of the absence of any evidence that Congress intended so intrusive a grant of authority, and for the reasons stated by Justice Holmes [in *American Tobacco*], . . . we think that the RTC must have at least an articulable suspicion that a former officer or director is liable to the failed institution before a subpoena for his personal financial information may issue.[123]

This did not require a showing of unlawful conduct, but "the degree of suspicion that attaches to particular types of noncriminal acts."[124]

And, apropos of bulk data surveillance, courts are stricter yet when the government seeks information about people who are not suspected of any criminal conduct, even if they have an intimate association with someone properly subject to investigation. The Second Circuit, in *In re McVane*, explained, "A person does not involve him or herself in matters foreseeably the object of agency inquiry simply by being a member of another's family."[125] When there is conjugal or familial association alone, a more "exacting scrutiny" is appropriate in which the agency must "make some showing of need for the material sought beyond its mere relevance to a proper investigation."[126]

Finally, and obviously, courts repeatedly emphasize that subpoenas, issued by all sorts of governmental actors, still and always are subject to judicial scrutiny. At such a hearing, the recipient "may challenge the summons on any appropriate ground."[127]

1144 (9th Cir. 1997) (discussing *In re* McVane, 44 F.3d 1127, 1138–39 (2d Cir. 1995) (finding the FDIC's subpoenas to be too broadly drawn)); FTC v. Turner, 609 F.2d 743, 745–46 (5th Cir. 1980) (same with respect to the FTC).

122 *Resol. Tr. Corp.*, 18 F.3d at 947.

123 *Id.* at 949.

124 *Id.*

125 *In re* McVane, 44 F.3d at 1138.

126 *Id.*

127 Reisman v. Caplin, 375 U.S. 440, 449 (1964); *see also In re* Subpoenas Duces Tecum Nos. A99-0001, A99-0002, A9900-3 & A99-0004, 51 F. Supp. 2d 726, 738 (W.D. Va. 1999) (litigant challenging subpoenas issued by the USAO); United States v. Tobins, 512 F. Supp.

In short, even though the government has incredibly broad subpoena power to collect information in aid of criminal investigations, including personal information, and even though no warrant or probable cause is required, the "reasonableness" clause of the Fourth Amendment imposes a set of regulatory requirements before such collection can occur. To be "reasonable" and thus constitutional under the Fourth Amendment, the government must have (1) formal authorization from the regulatory scheme; (2) a legitimate government purpose; and (3) the relevance of the information sought must relate to that legitimate purpose. Further, (4) there must be guardrails in place, such as requiring a greater showing of necessity when the particularly private information of individuals—rather than corporate information—is at stake, especially if those individuals are accused of no misconduct themselves. Finally, (5) courts are available to ensure these rules are followed. This is precisely the framework needed for bulk collection of surveillance data, and it is not being followed today. (Because subpoenas can be challenged in court, they of course meet the sixth prerequisite, of a regularized process for obtaining the information).

B. The Fifth Amendment and Required Records

Next, we turn to the Fifth Amendment. It is implicated in any number of situations in which the government collects personal information, but one in particular—the "required records" doctrine—demonstrates the necessity of regulatory prerequisites prior to government gathering personal data. The government often requires its subjects to maintain records of a variety of transactions. It may require reporting on those transactions to the government, as is familiar under tax laws. Or, it may subpoena that information at a later date. The question is: What must occur before the government makes these demands?

The seminal case here is *Shapiro v. United States*, a hotly contested 5–4 decision in which the majority held that the government could, without running afoul of the Fifth Amendment, subpoena records that an individual was required to maintain.[128] Shapiro was a fruit and vegetable merchant subject to the Emergency Price Control Act, which required him to keep certain records of his trade. He did, and complied with a subpoena to produce these records to enforcement attorneys of the Office of Price Administration. This in turn led to his being indicted for violating the Act, at which point he argued,

308, 310 (D. Mass. 1981) (litigant challenging a subpoena issued by the Department of Energy).

[128] 335 U.S. 1, 32–33 (1948).

inter alia, the compelled retention and production of documents violated the Fifth Amendment.[129]

The Court resolved the Fifth Amendment question against Shapiro, adopting what is known today as the "required records" doctrine. The Court concluded that the records were "public documents, which the defendant was required to keep, not for his private use, but for the benefit of the public, and for public inspection."[130] Were this not the case—were the documents "private papers"—then the privilege would have applied.[131]

The "required records" rule could have put a big dent in Fifth Amendment rights, but the rule was limited severely in *Marchetti v. United States*, which, when read alongside *Shapiro*, establishes important bounds on government collection of private information.[132] These required records cases identify the same prerequisites to government information collection we saw under the Fourth Amendment subpoena cases. Indeed, because of the Fifth Amendment interests at stake, they are applied even more rigorously.

First, the government simply cannot go demanding information—which is to say either requiring it be kept in the first instance, or that it be provided in response to a subpoena—without statutory authorization. In *Shapiro*, the Court explained its conclusion, beginning, "The record involved in the case at bar was a sales record required to be maintained under an appropriate regulation . . . ."[133] It stated that its rule would not apply to information "whose keeping as records has *not* been required by valid statute or regulation."[134]

Second (and third), there were again requirements of both a legitimate purpose and a connection of "relevance" between the statutory scheme and the information the government was collecting. In Shapiro's case, "its relevance to the lawful purpose of the Administrator is unquestioned."[135] His business records would indicate whether he was in fact complying with the terms of the Emergency Price Control Act. "[T]here is a sufficient relation between the activity sought to be regulated and the public concern so that the government can constitutionally regulate or forbid the basic activity concerned, and can constitutionally require the keeping of

---

129 *See id.* at 3–5, 5 n.3.

130 *Id.* at 17–18 (quoting Wilson v. United States, 221 U.S. 361, 381 (1911)).

131 *See id.* at 17.

132 390 U.S. 39, 41–42 (1968).

133 *Shapiro*, 335 U.S. at 35.

134 *Id.* at 27.

135 *Id.* at 35.

particular records . . . ."[136] On the other hand, the government could not require turning over data if it is "plainly incompetent or irrelevant to any lawful purpose."[137]

Fourth, turning to guardrails, *Marchetti* made clear that requiring recordkeeping was impermissible if the government's sole purpose was establishing criminal liability. *Marchetti* distinguished *Shapiro* because there the information requirements were imposed in "an essentially non-criminal and regulatory area of inquiry."[138] The gambling tax rules were invalid because "the statutory obligations are directed almost exclusively to individuals inherently suspect of criminal activities."[139]

Finally, in each of these cases the government's effort to collect data was by lawful process, subject to judicial review. Which is to say the government did not simply come and take the information: The information either was collected pursuant to duly enacted law or was collected by a statutorily authorized subpoena, or both. And the legality of that order was subject to judicial scrutiny. The collection could have been challenged before complying with the government order, or at the time the information was used in a criminal prosecution.[140] But in either event the collection itself was subject to judicial review.

C. "The Right to Be Let Alone"

Next, we will look at cases involving informational privacy rights under the Fourteenth Amendment. The cases thus far have involved investigations into individuals. In some of the next cases, the collection applied to many people, much like mass data collection.

There is some skepticism regarding the future viability of the right to privacy cases, but that skepticism seems unwarranted around information privacy.[141] The so-called privacy cases actually lump together two quite unrelated sorts of interests. One, implicated in

---

[136] *Id.* at 32.

[137] *Id.* at 30 (quoting Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943)).

[138] Marchetti v. United States, 390 U.S. 39, 57 (1968) (quoting Albertson v. Subversive Activities Control Bd., 382 U.S. 70, 79 (1965)); *accord* Grosso v. United States, 390 U.S. 62, 67–68 (1968).

[139] *Grosso*, 390 U.S. at 68 (discussing *Marchetti*, 390 U.S. 39).

[140] *Compare Marchetti*, 390 U.S. at 40–41 (reviewing conviction for failure to comply with the gambling business registration and occupational tax statute), *with Shapiro*, 335 U.S. at 3–5 (reviewing challenge to use of compelled documents).

[141] *See, e.g.*, Mary D. Fan, *Constitutionalizing Informational Privacy by Assumption*, 14 U. Pa. J. Const. L. 953, 981 (2012) (noting the continued uncertainty around the future of right to informational privacy).

cases like *Roe v. Wade*[142] and *Griswold v. Connecticut*, is independence in "making certain kinds of important decisions."[143] The other—implicated in the cases discussed below and in government surveillance—is "avoiding disclosure of personal matters."[144] There is controversy in the country regarding the first set of interests, but much less around the second. Numerous cases have accepted the existence of an informational privacy right—at least arguendo—and concluded that the very same regulatory prerequisites applied as in the other examples we have seen thus far.[145]

The informational privacy cases emerged at a time of great concern regarding the computerization of data and the questions about government power and individual autonomy that databases brought to the fore. In one of the early privacy cases, *United States v. Westinghouse Electric Corp.*, the Court explained how "one of the most fundamental and cherished rights of American citizenship," what Justice Brandeis had called "the right to be let alone," was being threatened by the "[p]roliferation in the collection, recording and dissemination of individualized information" in computerized "data banks."[146]

---

142 381 U.S. 479 (1965).

143 Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 144–45 (2011) (quoting Whalen v. Roe, 429 U.S. 589, 599–600 (1977) and drawing this very distinction).

144 *Whalen*, 429 U.S. at 599.

145 *See, e.g.*, Paul P. v. Verniero, 170 F.3d 396, 398, 400–01, 403, 405 (3d Cir. 1999) (performing *Whalen* analysis and upholding sex offender registry); Russell v. Gregoire, 124 F.3d 1079, 1081, 1089, 1094 (9th Cir. 1997) (same); Nat'l Treasury Emps. Union v. U.S. Dep't of the Treasury, 25 F.3d 237, 239, 242–44 (5th Cir. 1994) (performing *Whalen* analysis and concluding that the IRS could collect and store information of employees' drug use); Haw. Psychiatric Soc'y v. Ariyoshi, 481 F. Supp. 1028, 1033, 1037–38, 1040–41, 1043, 1045 (D. Haw. 1979) (performing *Whalen* analysis and upholding injunction against Hawaii state officials from gaining access to the records and offices of Medicaid providers); Norman-Bloodsaw v. Lawrence Berkeley Lab'y, 135 F.3d 1260, 1264, 1269, 1270 (9th Cir. 1998) (holding that the collection of private genetic information from public sector employees who only consented to a general health examination violates constitutional right to privacy); *Nat'l Aeronautics & Space Admin.*, 562 U.S. at 139–41, 150–52, 154–56, 159 (2011) (performing *Whalen* analysis and concluding that NASA's collection of information regarding employee drug use or counseling for drug use did not violate constitutional right to privacy); Fraternal Ord. of Police, Lodge No. 5 v. City of Philadelphia, 812 F.2d 105, 107, 110, 112, 116–18 (3d Cir. 1987) (performing *Whalen* analysis to determine whether the use of a questionnaire to collect information on police applicants' mental health, physical health, finances, drug use, and arrest records violated constitutional right to privacy); Statharos v. N.Y.C. Taxi & Limousine Comm'n, 198 F.3d 317, 319, 322–23, 325–27 (2d Cir. 1999) (performing *Whalen* analysis and upholding a NY statutory scheme to collect financial information of NYC taxi medallion owners).

146 United States v. Westinghouse Elec. Corp., 638 F.2d 570, 576 (3d Cir. 1980). *See generally* Slobogin, *supra* note 48, at 239 (discussing Peter Westin's seminal study in this period describing privacy as an individual's expectation that they can behave as if they are not being watched). As a result, Congress passed the Privacy Act of 1974, 5 U.S.C. § 552a (as amended) which was foremost on the Justices' minds, even if it did not resolve the

Two 1977 cases signaled the constitutional protection of informational privacy; one involved Richard Nixon's private papers, the other was *Whalen v. Roe.*[147] Whalen involved a challenge to a New York statute requiring physicians to report and New York to store information regarding the prescribing and dispensing of controlled drugs.[148] Plaintiffs argued the law violated the constitutional right to privacy, a right the Court fully acknowledged, even while upholding New York's requirements.[149] Nixon's lawsuit challenged a congressional statute that took control of his papers and provided for archiving, eventual release, and—notably—careful separation of his purely private papers from the rest.[150] Nixon argued the law violated the Constitution in numerous ways, from separation of powers to the Fourth Amendment, but the District Court deemed the privacy claim "[t]he most troublesome challenge that plaintiff raises."[151]

In the informational privacy cases, the Supreme Court's starting place once again is the requirement of prior legislative authorization to collect the information. New York's law challenged in *Whalen*, the Court explained, "is manifestly the product of an orderly and rational legislative decision."[152] In resolving Nixon's suit, the Court stated that the "claim of invasion of his privacy cannot be considered in the abstract; rather, the claim must be considered in light of the specific provisions of the Act."[153] *Westinghouse* involved a subpoena for information; unlike the subpoena cases discussed above, however, the request was not for company information but for private health information of the company's employees in order to assess a risk from exposure to certain chemicals.[154] Following the doctrine of the subpoena cases, and citing specifically to *Morton Salt*, first up on the Court's analysis was that "the inquiry must be within the authority of the agency."[155] To this end, it consulted the Occupational Safety and Health Act of 1970, which authorized the Secretary to "make inspections," "question employers," and "issue subpoenas to obtain the production of evidence."[156]

---

constitutional challenges to the collection and aggregation of data the Court faced. The Act established rules for collection, management, and use of private data. But the law only applied to the federal government, and even then, had an exception for law enforcement.

147 *Whalen*, 429 U.S. 589; Nixon v. Adm'r of Gen. Servs., 433 U.S. 425 (1977).

148 *See Whalen*, 429 U.S. at 591–94.

149 *See id.* at 599–600, 603–04.

150 See *Nixon*, 433 U.S. at 433–36, for a detailed discussion of the statute in question.

151 Nixon v. Adm'r of Gen. Servs., 408 F. Supp. 321, 357 (D.D.C. 1976).

152 *Whalen*, 429 U.S. at 597.

153 *Nixon*, 433 U.S. at 458.

154 United States v. Westinghouse Elec. Corp., 638 F.2d 570, 573 (3d Cir. 1980).

155 *Id.* at 574.

156 *Id.* at 575.

Then, the Court turned to the questions of justification and whether the statutory scheme furthered the legislative purpose. Despite the fact that the *Whalen* Court upheld the law, it nonetheless engaged in a careful analysis of the various state interests that supported the collection of drug prescription information.[157] Had there been no interests at stake, or had the information not furthered them, it would be hard to see the law being upheld.[158] The same was true in the *Nixon* case: The law was "a reasonable response to the difficult problem caused by the mingling of personal and private documents" with nonprivate ones in the face of "government interests of overriding importance."[159]

Given that informational privacy is at stake, the cases focus particularly closely on guardrails. Echoing the special rule under the Fourth Amendment for the subpoena of private information, the Court typically adds a step in privacy cases, balancing the government interest furthered by the law against the individuals' privacy interest.[160] For example, because private medical records were at issue in *Westinghouse*, the Third Circuit said it "must engage in the delicate task of weighing competing interests."[161] Similarly in *Nixon*, "any intrusion must be weighed against the public interest."[162]

As for specific guardrails, the Court pays close attention to the degree that the statutory scheme—including any implementing regulations—minimizes the intrusion on, and safeguards, the private information at stake.[163] In upholding the statute taking control of Nixon's papers, the Justices compared the law to the provisions of the federal wiretap act, which imposes safeguards to allow access to information investigators require while protecting "private communications unconnected with any legitimate government objectives."[164] In

---

157 *See Whalen*, 429 U.S. at 597–98 (discussing how the statute at issue might aid in the enforcement of laws designed to minimize the misuse of dangerous drugs).

158 *See also* Nat'l Treasury Emps. Union v. U.S. Dep't of Treasury, 25 F.3d 237, 242–44 (5th Cir. 1994) (discussing, in depth, the validity of the "public trust" justification the Treasury Department gave in collecting information about the use of drugs and alcohol by its employees).

159 Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977).

160 *See, e.g.*, Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 138 (2011) (balancing the government's interest in collecting information with individuals' interest in avoiding disclosure); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) (same); Fraternal Ord. of Police, Lodge No. 5 v. City of Philadelphia, 812 F.2d 105, 112–17 (3d Cir. 1987) (same).

161 United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).

162 *Nixon*, 433 U.S. at 458.

163 *See, e.g.*, McKenna v. Fargo, 451 F. Supp. 1355, 1381–82 (D.N.J. 1978) (noting that regulations collecting data are more justified when "narrowly drawn" and "securely safeguarded from improper access").

164 *Nixon*, 433 U.S. at 463.

Nixon's case, there were no "less restrictive means" to avoid separating commingled documents.[165] In *Westinghouse*, although the balance favored release of the information to the government, given that "there may be information in a particular file which an employee may consider highly sensitive," the Court mandated that the government "give prior notice to the employees whose medical records it seeks to examine and to permit the employees to raise a personal claim of privacy, if they desire."[166] The *Whalen* Court expressed concern for securing private data to ensure it only was available for authorized, pre-approved uses. It detailed at length the security provisions for the data at issue in that case, including the existence of criminal liability for disclosing information, the very limited number of employees with access to the data, and that when the data was accessed, the system was run "off-line" so "no terminal outside of the computer room can read or record any information."[167] Given "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files," the Court made clear it was not deciding any question involving "a system that did not contain comparable security provisions."[168]

In short, and once again, before obtaining personal information, the government must have statutory authorization, a valid government purpose, and a nexus between the information collected and that legitimate purpose. And when private information is at stake, there must be particular safeguards to (1) minimize any intrusion; and (2) assure adequate security for the information.[169] Lawful process to obtain the information was found in the statutes that mandated collection, or in the subpoena to acquire it. All of this was subject to judicial review.[170] Nixon, the Supreme Court emphasized, was guaranteed "full judicial review before any public access [was] permitted."[171]

D. The First and Second Amendments

At the risk of sounding like a broken record, the Supreme Court imposes a very similar set of legal prerequisites when personal information collection is challenged under yet additional provisions of the

---

165 *Id.* at 427, 464.

166 *Westinghouse Elec. Corp.*, 638 F.2d at 580–81.

167 Whalen v. Roe, 429 U.S. 589, 594 (1977).

168 *Id.* at 605–06; *accord id.* at 606–07 (Brennan, J., concurring).

169 *See id.* at 596–98, 601 (majority opinion); *see, e.g.*, Haw. Psychiatric Soc'y, Dist. Branch of Am. Psychiatric Ass'n v. Ariyoshi, 481 F. Supp. 1028, 1043 (D. Haw. 1979) (noting these two aspects of the balancing test).

170 *See Whalen*, 429 U.S. at 597–98 (evaluating the rational basis for the challenged statute).

171 Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 467 (1977).

Constitution. Here we see the same under the First Amendment—and even the Second.

The state often seeks information about people's associational ties, and not infrequently, the request for information is challenged as interfering with First Amendment rights of association. The seminal First Amendment associational rights case is *NAACP v. Alabama*, in which the State of Alabama sought access to the NAACP's membership records.[172] The opinion, written at the height of the civil rights movement and denying the State of Alabama the access it sought, is not a paradigm of clarity. Still, the reason Alabama lost touches on the various prerequisites: a statute authorized the collection, but the state's purported interest did not justify the collection; not only were there insufficient safeguards for the information, but when this sort of information was disclosed—the Court pointed out—individuals regularly were subjected to harassment.[173] *NAACP v. Alabama* spawned a host of First Amendment cases that, if not identical, were similar in nature, all of which were increasingly clear about the various prerequisites.[174] There also are grand jury cases raising First Amendment issues that, like other subpoena cases, follow the same formula.[175]

---

[172] 357 U.S. 449 (1958).

[173] *See NAACP*, 357 U.S. at 452 (noting Alabama's foreign corporation registration statute authorized the collection); *id.* at 464–66 (holding that Alabama's interest in obtaining the membership lists—to ascertain if the NAACP was conducting intrastate business in violation of the statute—did not justify the collection); *id.* at 462–63 (describing types of harassment NAACP members faced when their identities were disclosed).

[174] *See, e.g.*, Shelton v. Tucker, 364 U.S. 479, 484–90 (1960) (striking down an Arkansas statute compelling teachers to disclose organizational ties by relying on all above factors, especially a lack of safeguards, and holding that "the unlimited and indiscriminate sweep of the statute . . . goes far beyond what might be [legitimately] justified"); Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 546–58 (1963) (reviewing special committee's order for the president of local NAACP to bring membership records by relying on all above factors, particularly an insufficient relationship between government interest and the collection); United States v. Citizens State Bank, 612 F.2d 1091, 1093–94 (8th Cir. 1980) (reversing District Court for not considering above factors in review of IRS subpoena); Fed. Election Comm'n v. Larouche Campaign, 817 F.2d 233, 234–35 (2d Cir. 1987) (modifying subpoena where the FEC only demonstrated a sufficient justification for part of the collection request); Loc. 1814, Int'l Longshoremen's Ass'n, AFL-CIO v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267, 271–74 (2d Cir. 1981) (modifying subpoena to limit disclosure of contributor names by relying on above factors, in particular legitimate interest and safeguards); Hotel Emps. and Rest. Emps. Int'l Union v. Nev. Gaming Comm'n, 984 F.2d 1507, 1517–18 (9th Cir. 1993) (upholding subpoena based on above factors and holding that "the disclosure requirements are substantially related to the compelling government interests in protecting the free and honest conduct of gaming . . . and they are narrowly tailored to affect only a limited group").

[175] *See, e.g.*, *In re* First Nat'l Bank, Englewood, Colo., 701 F.2d 115, 117–19 (10th Cir. 1983) (remanding order compelling production of anti-tax groups' bank accounts and review of the collection in light of all factors above, particularly whether the collection could be minimized); *In re* Grand Jury Proc. v. United States, 776 F.2d 1099, 1102–04 (2d Cir. 1985) (upholding subpoena for testimony by a Hells Angels member about the group

The October 2020 Term First Amendment decision in *Americans for Prosperity Foundation v. Bonta* (AFP) is exemplary; it covered the entire range of prerequisites.[176] In *Americans for Prosperity*, by a 6–3 vote, the Supreme Court struck down a regulation adopted by the California Attorney General requiring all charities to disclose the names and addresses of major donors.[177] The regulation was pursuant to a statute.[178] The Court identified the justification for requesting the information: "preventing wrongdoing by charitable organizations."[179] Yet, although "[i]t goes without saying that there is a 'substantial governmental interest[] in protecting the public from fraud,' . . . [t]here is a dramatic mismatch between the interest that the Attorney General seeks to promote and the disclosure regime that he has implemented in service of that end."[180] Relevant to the bulk collection of surveillance data, the majority was critical of the volume of information required vis-à-vis its utility: "The upshot is that California casts a dragnet for sensitive donor information from tens of thousands of charities each year, even though that information will become relevant in only a small number of cases involving filed complaints."[181] That did not obviate the utility of the information, but there were countervailing associational and "privacy concerns."[182] The Justices also were extremely skeptical that the regulatory scheme contained sufficient safeguards, pointing to the Attorney General's erroneous posting of information on its website and quoting the trial court as to "the amount of careless mistakes made by the Attorney General's Registry is shocking."[183] Finally, not only was judicial review available

after analysis of above factors); *In re* Grand Jury Subpoenas Duces Tecum, 78 F.3d 1307, 1312 (8th Cir. 1996) ("A grand jury subpoena will be enforced despite a First Amendment challenge if the government can demonstrate a compelling interest in and a sufficient nexus between the information sought and the subject matter of its investigation.").

176 141 S. Ct. 2373 (2021).

177 *Id.* at 2379.

178 *Id.* at 2379–80.

179 *Id.* at 2385–86.

180 *Id.* at 2386. In reaching this conclusion the Court applied "exacting scrutiny." *Id.* at 2383. The level of scrutiny was itself a point of contention among the Justices. *See id.* at 2390 (Thomas, J., concurring) (advocating for strict scrutiny); *id.* at 2391–92 (Alito, J., concurring) (declining to decide a level of scrutiny); *id.* at 2396 (Sotomayor, J., dissenting) (arguing that the majority's use of "exacting scrutiny" is less flexible than the standard was historically). In various contexts across the amendments discussed here, the courts apply different levels of scrutiny. *E.g.*, NAACP v. Alabama, 357 U.S. 449, 461 (1958) ("closest scrutiny"); *AFP*, 141 S. Ct. at 2383 ("exacting scrutiny"). But no matter what the level of scrutiny, courts always return to the same set of requisite factors.

181 *AFP*, 141 S. Ct. at 2387.

182 *Id.* at 2388.

183 *Id.* at 2381 (internal quotation marks omitted); *see also id.* at 2388 n.* ("Here, the State's assurances of confidentiality are not worth much.").

before collection was mandated, but the Court took the somewhat extreme step of entertaining a facial challenge to the statute, given the fact that the collection regime was not "narrowly tailored" but swept so broadly.[184]

The very same requisites are addressed in Second Amendment cases involving the collection of personal information. Two decisions from the D.C. Circuit make the case. *National Rifle Association v. Reno* involved a challenge to a decision by the Attorney General to retain temporarily some information required of people during background checks to acquire guns, in order to use the information for auditing purposes.[185] In a 2–1 decision, the judges disagreed on the question of whether the statute authorized this temporary retention, underscoring the importance of the authorization issue.[186] Although for the most part it was a case of textual statutory interpretation, the majority opinion upholding the Attorney General's decision showed how auditing would help fulfill the underlying purpose of the statute, and in particular would confirm that statutory safeguards on the collection of the information were not being abused.[187] *Heller v. District of Columbia* was a case challenging certain registration provisions of D.C.'s gun law adopted after the Supreme Court had invalidated an earlier version.[188] Statutory authorization was a given, but what is notable about *Heller* is the care the Court took to determine the justification for the registration provisions (which included appearing in person to provide fingerprints and producing the registered weapon), and whether the statutory requirements actually furthered that purpose.[189] Again in a 2–1 decision (the dissenting judge would have upheld all the provisions), the majority parsed the record evidence to approve of some registration requirements but strike down others.[190] This underscores that both a justification and proof that the collecting

184 *Id.* at 2385–89.

185 216 F.3d 122, 124–25 (D.C. Cir. 2000).

186 *See id.* (holding that nothing in the Brady Act prohibited the temporary retention of the data); *id.* at 138–39 (Sentelle, J., dissenting) (arguing that the Attorney General exceeded the authority granted to her under the statute).

187 *See id.* at 133 (majority opinion) ("[T]he Attorney General uses the Audit Log to accomplish the very purpose of the Gun Control and Brady Acts, i.e., to ensure that individuals not authorized to possess firearms are unable to purchase them.").

188 801 F.3d 264 (D.C. Cir. 2015).

189 The Court cited numerous sources on the efficacy of the provisions, including a report by the U.S. Government Accountability Office indicating that the fingerprinting requirement would "help to deter and detect fraud" and a report by the Committee of the Judiciary emphasizing that the photograph requirement was essential to "quickly identify whether and to whom the firearm has been legally registered." *Id.* at 276.

190 *Id.* at 280–81 (majority opinion); *id.* at 281 (Henderson, J., concurring and dissenting in part).

of information will further the justification are necessary. In short, under both the First and Second Amendments the by-now familiar prerequisites are relied upon by courts before the government can collect personal information.

E. Back to the Fourth: Special Needs

Before moving on, a quick return to the Fourth Amendment is in order, and specifically to the topic of "special needs" searches. Special needs searches are those in which the government is pursuing "special needs, beyond the normal need for law enforcement."[191] I treat them here, because many of them are—unlike subpoena cases—programmatic, i.e., they involve the collection of information from many people, and without any individualized suspicion. They thus are akin to the very sort of unregulated government gathering of surveillance information with which I am concerned. Examples of special needs include checking in on probationers and parolees to make sure they are adhering to conditions of release, maintaining sobriety checkpoints, and drug testing students or employees *en masse*.[192]

The treatment of special needs searches under the Fourth Amendment bookends the treatment of subpoenas under the same Amendment, in that in neither case does the finding that something is a "search" trigger a probable cause or warrant requirement; rather, in each case a specialized test invokes the prerequisites of personal information collection. Under the special needs doctrine, government programmatic generalized searches and seizures are permissible, so long as (a) the government interest outweighs that of individuals; (b) the program has "adequate safeguards" to substitute for a warrant and cause; and (at least in some of the cases) (c) the program is efficacious.[193]

As the Supreme Court's reasoning in *Skinner v. Railway Labor Executives' Association* demonstrates, although the special needs doctrine is formulated as a three-part test, in application the analysis often aligns quite precisely with the prerequisites analysis we have

---

[191] *See* Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) ("Although we usually require that a search be undertaken only pursuant to a warrant . . . we have permitted exceptions when 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'" (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring))).

[192] *See, e.g.*, *Griffin*, 483 U.S. 868 (supervision of probationers); Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (sobriety checkpoints); Skinner v. Ry. Lab. Exec. Ass'n, 489 U.S. 602 (1989) (drug testing railway employees); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989) (drug testing Customs Service employees).

[193] *See Sitz*, 496 U.S. at 449–50 (setting out three-part test for special needs searches).

been discussing.[194] *Skinner* involved a challenge to certain federal regulations authorizing breath and urine tests of railway employees for impairment from drugs and alcohol following accidents, and also allowing for some random testing.[195]

In upholding the drug-testing program, the *Skinner* Court identified every single prerequisite as crucial to its conclusion. The substance testing program was statutorily authorized, and regulations had been promulgated by the Federal Railroad Administration to support it.[196] Repeatedly the Court pointed to the justifications of investigating railroad accidents, and deterring substance use by workers, and explained how the drug-testing program met them.[197] The Court upheld the program because it furthered these purposes.[198] The tests were only conducted pursuant to specifically defined statutory procedures.[199] In light of the personal privacy interests at stake, there were a variety of safeguards in place; among them, either everyone must be tested to avoid officer discretion as to who was tested, or there must be individualized cause as to a particular person.[200] Penalties attached to those who violate the regulations.[201] Finally, quite obviously, the program was subject to judicial review.

Admittedly, in some of the special needs cases, courts can get sloppy about parts of the prerequisite analysis, no doubt because the Court's three-part stated test is not specific enough about all six requirements. Thus, although in most of its special needs cases the Supreme Court identifies the statutory or regulatory authority of the body adopting the search program—be it a school board, a legislative body, or an agency—the Court did uphold a sobriety checkpoint set up by a policing agency with no such authorization.[202] Interestingly, some state courts have caught the Supreme Court's error and specifically struck down sobriety checkpoints that lacked statutory authori-

194 489 U.S. 602 (1989).
195 *Id.* at 609–11.
196 *Id.* at 606.
197 *Id.* at 621–22, 628–29.
198 *Id.* at 633–34.
199 *Id.* at 622.
200 *Id.* at 622 n.6.
201 *Id.*
202 *Compare Skinner*, 489 U.S. 602 (upholding Federal Railroad Administration drug testing program adopted under the "Secretary of Transportation's statutory authority to adopt safety standards for the industry"), *and* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (upholding student drug testing program adopted under the authority of the school district board), *and* Griffin v. Wisconsin, 483 U.S. 868 (1987) (upholding a scheme providing for the warrantless search of probationers' homes authorized by State Department of Health and Social Services regulation), *with* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (upholding a sobriety checkpoint pilot program established by the Michigan Department of State Police absent legislative authorization).

zation.[203] Similarly, the Justices often fight among themselves about whether the search program at issue actually furthers the government's stated purpose.[204] Even here, though, this is clear acknowledgment that such a prerequisite of furthering a legitimate governmental purpose exists.

In short, once again under the Fourth Amendment itself, the Supreme Court—and state courts—allow special needs searches, but only if they satisfy a version of the same prerequisites seen in other cases involving the collection of private information. There is no need for a warrant and probable cause in these searches. Rather, the focus is on regulatory prerequisites.

III
The Requisites of Surveillance Data Collection

By now we've seen in almost tiresome detail that courts typically impose some very familiar prerequisites as a predicate to government collection of private data on individuals. Part IV will set out the constitutional basis for doing the same in the context of government surveillance data collection. Before turning to the constitutional question, though, this Part examines in detail how those prerequisites should apply to surveillance data collection. What will become clear is how far current practice around surveillance data collection strays from what appropriate application of the prerequisites would require. That is what must change.

A. Authorization

It's hardly surprising that the overridingly common element in the cases discussed above was the Court assuring itself that an appropriate legislative or regulatory body had authorized executive officials to collect the personal information. It is bedrock constitutional and administrative law that agency action must be authorized legislatively,

---

[203] *See, e.g.*, Nelson v. Lane Cnty., 743 P.2d 692 (Or. 1987) (holding that broad statute describing duty of state police agency did not authorize sobriety roadblocks); State v. Sims, 808 P.2d 141 (Utah Ct. App. 1991) (holding sobriety roadblocks unlawful absent statutory authorization).

[204] *See, e.g.*, *Skinner*, 489 U.S. at 636 (Marshall, J., dissenting) (accusing the majority of "overlooking serious conceptual and operational flaws in the FRA's testing program" that "cast grave doubts" on the majority's characterization of the program's effectiveness); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 686 (1989) (Scalia, J., dissenting) (disagreeing with the majority's contention that the Customs Service's drug testing program deters drug use by Service personnel, and arguing that "there is only a slight chance that it will prevent some serious public harm resulting from Service employee drug use").

or it is ultra vires.[205] Too often, when government surveillance is at issue, courts skip immediately to the question of whether such surveillance violates a constitutional right. That drags the constitutional cart before its horse. The proper first constitutional question is not what is prohibited to government, but what the executive branch is permitted to do. Are executive officials—including the police—authorized to do what they are doing?[206]

To the extent government policing agencies are collecting personal data without authorization, it is impermissible. Oregon, for example, is one of many states whose fusion center has no legislative authorization whatsoever.[207] Housed in Oregon's Department of Justice, under a bureau authorized only to investigate "organized crime," the Oregon Terrorism Intelligence and Threat Assessment Network (TITAN) Fusion Center collects and aggregates information on countless individuals, including Black Lives Matter protesters, anti-Trump protesters, and environmental activists.[208] No statute authorizes such conduct.[209]

The authorization question is more complicated than the fusion center example suggests, though, because most policing agencies are not acting in the absence of any authorization whatsoever. Typically, such agencies have—at a minimum—a chartering statute that states very generally what they may do (and thus, implicitly, what they may

[205] *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. 2014) ("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.").

[206] *Supra* note 205 and accompanying text.

[207] *See* MICHAEL GERMAN & JAY STANLEY, ACLU, WHAT'S WRONG WITH FUSION CENTERS? 6 (Dec. 2007), https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf [https://perma.cc/7WWT-ZLU3] (describing how fusion centers developed "in the absence of any legal framework" for regulating their activities).

[208] *See* Parrish & Wilson, *supra* note 67 (environmental activists); Eder Campuzano, *Homeland Security Characterizes Portland's Anti-Trump Riot as 'Terrorist Violence:' Report*, THE OREGONIAN (Mar. 3, 2017, 2:25 AM), https://www.oregonlive.com/portland/2017/03/homeland_security_calls_portland_trump_riot_domestic_terrorist_violence.html [https://perma.cc/G6JA-H6HV] (anti-Trump protesters); Amanda Peacher, *Why Is the State of Oregon Conducting Intelligence Work?*, OR. PUB. BROAD. (Apr. 26, 2016, 8:00 AM), https://www.opb.org/news/article/oregon-department-of-justice-intelligence [https://perma.cc/6FE3-7AWZ] (BLM protesters).

[209] I am one of a team of lawyers challenging the legality of Oregon's fusion center on these grounds.

not).[210] It often grants the agency authority to do something like "enforce the law, keep the peace, and maintain order."[211]

The question then is, how specific and timely must an authorization be with regard to surveillance data collection? Are very broad authorizations of what police may do carte blanche for any means to pursue that end? Are charters adopted many decades ago sufficient to authorize the use of technologies unimaginable even a short time ago to engage in mass data collection?

It turns out this sort of question is not unfamiliar, even around data collection for policing. An early example arose in the context of whether police could collect fingerprints, photographs, and Bertillon measurements of people accused of crimes. *Gow v. Bingham* was a 1907 New York Supreme Court case involving an individual indicted on charges of grand larceny and forgery.[212] He moved for a mandamus to compel destruction of records such as fingerprints he claimed were taken from him unlawfully. The *Gow* court found that "[n]o statute has been found which, in express terms, authorizes any member of the police force" to take the photographs and measurements simply because someone was charged with a crime.[213] The court specifically rejected the police department's argument that it had "implied authority" flowing from the charter charging the police both to "especially preserve the public peace, prevent crime, and detect and arrest offenders" and to promulgate rules to effectuate doing so.[214] "The act of determining whether the liberty of a citizen shall be infringed, in the manner above referred to, belongs solely to the Legislature."[215]

To be sure, there were cases that went exactly the opposite way of *Gow*, the primary basis for which seemed to be the widespread acceptance of the practice at the time the case arose. Two years after *Gow*, the Maryland Court of Appeals upheld similar recording of persons, under a broad grant of authority to the police "to preserve the public peace, prevent crime, arrest offenders, and protect the rights of

---

210 *See* Friedman & Ponomarenko, *supra* note 14, at 1884 (noting that policing agencies typically are authorized by "statutes of sweeping generality, typically adopted some time ago").

211 *See id.* at 1883 (providing examples of broad statutes authorizing police agencies).

212 107 N.Y.S. 1011 (Sup. Ct. 1907).

213 *Id.* at 1015.

214 *Id.* at 1015. The court was analyzing the New York City charter, adopted in 1897 by the New York State Legislature. Charter Revision Committee, *About Charter Revision Commissions*, CITY OF N.Y., https://www1.nyc.gov/site/charter/about/about-the-commission.page [https://perma.cc/B83J-SL4T].

215 *Gow*, 107 N.Y.S. at 1017.

persons and property."[216] The court was willing to "assume[] that the Legislature in the imposition of the duties intended also to confer the incidental powers necessary to their discharge."[217] Conceding contrary precedent, the court took notice of the fact that "it is the daily practice of the police officers and detectives of crime" to use these means "for the discovery and identification of criminals, and without such means many criminals would escape identification."[218]

Come the later part of the twentieth century, a similar debate played out over the police use of roadblocks, particularly sobriety checkpoints, which were a novelty of sorts at the time. The terms of the debate echoed its predecessor at the turn of the century. Some state courts approved roadblocks under general grants of authority, but others did not. The Utah Supreme Court held that "[a]lthough certain roadblocks are authorized by statute, at the time of the search in question Utah law did not expressly authorize suspicionless investigatory roadblocks."[219] Similarly, in *Nelson v. Lane County*, the Oregon Supreme Court held that the State Police's general powers to "prevent crime" and "pursue and apprehend offenders and obtain legal evidence necessary to insure the conviction in the courts of such offenders" would not support a sobriety checkpoint.[220] Because roadblocks were seizures, followed often by searches, "executive agencies must have explicit authority from outside the executive branch."[221]

It's hard to put a finger on the precise factors that lead courts to go one way or another on the authorization question. It often seems like a matter of taste, including factors that appear only in passing in the opinions, such as the extent of the intrusion, the concern about limits on police authority, or the widespread acceptance of the practice.[222] But whether courts find a particular police practice is authorized or not, these courts did the proper thing in analyzing whether there was authorization. In the typical case challenging surveillance data collection on constitutional grounds, courts never examine

---

216 Downs v. Swann, 73 A. 653, 655 (Md. 1909). The Maryland court was analyzing the Baltimore City Charter, enacted in 1898. *Id.*

217 *Id.*

218 *Id.* at 656.

219 Sims v. Collection Div. of the Utah State Tax Comm'n, 841 P.2d 6, 9 (Utah 1992).

220 743 P.2d 692, 695 (Or. 1987) (internal quotation marks omitted).

221 *Id.* at 695.

222 *See, e.g.*, Gow v. Bingham, 107 N.Y.S. 1011, 1017 (Sup. Ct. 1907) (concluding fingerprinting is an infringement of liberty despite how common the practice is); Downs v. Swann, 73 A. 653, 656 (Md. 1909) (concluding fingerprinting is common; limiting it would be a "matter of regret"); Hodgeman v. Olsen, 150 P. 1122, 1124 (Wash. 1915) (upholding reformatory's retention of photographs because taking and retaining photographs "is a measure adopted in nearly all penal institutions," and "[t]he Legislature is . . . presumed to have had this common knowledge when it passed the reformatory act").

whether the agency was authorized in the first place to conduct the surveillance it did. That, for example, is true of all the Fourth Amendment cases cited in Part I.

A rare and somewhat recent example of a court getting this right, however, was the Second Circuit's resolution of the ACLU's challenge to National Security Agency bulk data collection, *ACLU v. Clapper*.[223] In 2015, the Second Circuit ruled that the NSA's comprehensive collection of telephone metadata "exceeds the scope of what Congress has authorized," and thus managed to avoid the challenging Fourth Amendment question of whether such collection constituted a search.[224] We'll delve more deeply into Judge Lynch's opinion for the court in *Clapper* momentarily, but in terms of its approach—looking first to statutory authorization—it was right on the money.

B. Transparency

There's another prerequisite that we've not even had to pay attention to yet: transparency. By this I mean that the public is aware government is collecting this sort of personal information. Transparency is not even on the list of six prerequisites, because in every case discussed in Part II the government collection of personal information was open and notorious, as well as authorized. That only stands to reason: If the collection of information is authorized, people know it is happening. But when there is no authorization, there also is the risk of non-transparency.

There simply is no excuse for government covering up the means by which it keeps tabs on the public. It's true that individual investigations may need to occur in secret, but that is different from keeping an entire area of government conduct under wraps. Even in the area of foreign intelligence gathering, while investigations may be secret, the tools being used by government both are and must be known, at least to authorizing officials.[225] That was the point of the *Clapper* decision holding NSA metadata collection unauthorized.

It's simply impossible to authorize, or regulate, what one knows nothing about. As the *Clapper* court put it, "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."[226] An all-too-familiar pattern today is public discovery that the government

---

223 785 F.3d 787 (2d Cir. 2015).

224 *Id.* at 792.

225 *See* Bernard Horowitz, *FISA, the "Wall," and Crossfire Hurricane: A Contextualized Legal History*, 7 NAT'L SEC. L.J. 1, 19 (2020) (describing the requisites for FISA surveillance, including that the surveillance be to procure "foreign intelligence").

226 *Clapper*, 785 F.3d at 820.

is using some sort of surveillance technique, then a public uproar, and eventually either abandonment of the practice or appropriate regulation, be it by courts or legislative bodies. This has been true, for example, around cell site simulators, drones, and facial recognition.[227] The hostile reaction that disclosure engenders underscores that the techniques neither were authorized nor approved. As such, they should not have been used.

C. Justification

Authorization is not enough; there also has to be a reason for permitting the collection of surveillance information. This requirement of a justification was pervasive in the cases in Part II, whether the collection was individual (in the case, e.g., of subpoenas), or programmatic (such as drug testing).[228] That's hardly surprising: Constitutional law at bottom is about the giving of reasons.[229] Whether the burden on the government of proffering a justification is strong or weak typically depends on whether the government is infringing a fundamental right.[230] Whichever is the case, *some* justification is needed.

Authorization and justification are related in a way that can help in some cases to resolve the authorization question. If the justification offered by the government in support of what it is doing does not fall within the supposedly-authorizing charter language, there's a

---

[227] *See* Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, BALT. SUN TIMES (Apr. 9, 2015), https://www.baltimoresun.com/news/crime/bs-md-co-county-stingray-20150409-story.html [https://perma.cc/2MJP-7KZV] (cell site simulators); Laura L. Myers, *Seattle Mayor Grounds Police Drone Program*, REUTERS (Feb. 8, 2013), https://www.reuters.com/article/us-usa-drones-seattle/seattle-mayor-grounds-police-drone-program-idUSBRE91704H20130208 [https://perma.cc/PZ8G-XQMB] (drones); Hill, *supra* note 51 (facial recognition).

[228] A legitimate justification for data collection also is required by state courts. *See, e.g.*, O'Brien v. DiGrazia, 544 F.2d 543 (1st Cir. 1976) (finding that the state's interest in discovering and deterring police corruption justified requiring officers to complete financial questionnaires); Perkey v. Dep't of Motor Vehicles, 721 P.2d 50, 52 (Cal. 1986) (finding that the need to "ensure the accuracy" of DMV records and "verify the personal identification information contained in the licensing system" justified a fingerprinting requirement for driver's license applicants); State v. Williams, 761 S.E.2d 662, 666 (N.C. Ct. App. 2014) (finding that requiring sex offenders to enroll in a satellite monitoring program "is a legitimate nonpunitive governmental objective").

[229] *See, e.g.*, Richard H. Pildes, *Avoiding Balancing: The Role of Exclusionary Reasons in Constitutional Law*, 45 HASTINGS L.J. 711, 712 (1994) ("[C]onstitutional adjudication . . . is about defining the kinds of reasons that are impermissible justifications for state action in different spheres."); CASS R. SUNSTEIN, THE PARTIAL CONSTITUTION 17 (1993) ("In American Constitutional law, government must always have a reason for what it does.").

[230] *See* 2 RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW § 15.4(a) (updated in May 2021) ("If a law regulates the exercise of a 'fundamental right,' a court should give less deference to the legislature and independently scrutinize the law.").

problem. Take fingerprinting. The *Gow* court, in striking down the practice, referred back to New York's general chartering language for the police department.[231] As the court saw it, Gow already had been detected and arrested, and the public peace "cannot readily be disturbed by a man in the custody of the law."[232] In other words, the proffered justification did not fall within the agency's authorization. In *Downs*, by contrast, the police argued they needed to be able to identify the suspect if he escaped. The Maryland court saw this justification as within the authority granted the department: For "the agencies, charged with the duty of preserving the public peace and arresting persons reasonably suspected of the commission of crimes," it made sense that "a full description of him should be had in order that, if he should undertake to become a fugitive from justice, the police and detective department may be in possession of such information as will enable them to have him identified, wherever he may be found."[233]

The justification prerequisite applies whether personal information is collected individually (e.g., by way of subpoena) or *en masse*, but the ability of a legislative or regulatory body to justify mass surveillance might be complicated somewhat by the special needs rule we saw at the end of Part II, which permits data collection without warrant or probable cause only if it furthers needs outside those of ordinary law enforcement. The key case here is *City of Indianapolis v. Edmond*, involving a roadblock set up to interdict drugs flowing into neighborhoods where crime was spiraling because of narcotics trafficking.[234] In holding the roadblock unconstitutional, the Supreme Court distinguished its decision upholding a sobriety checkpoint in *Michigan Department of State Police v. Sitz*.[235] The Court's reasoning was that sobriety checkpoints furthered a "special need" at issue—to get impaired drivers off the roads—whereas the drug checkpoint was simply about enforcing the law against those carrying drugs.[236]

Edmond has not, however, limited all mass data collection: Deterrence, for example, has proven an acceptable "special need."[237] We saw that at work in the *Skinner* railroad drug-testing case. As the *Skinner* Court explained, "While no procedure can identify all

---

231 *See supra* notes 212–15 and accompanying text.

232 Gow v. Bingham, 107 N.Y.S. 1011, 1015 (Sup. Ct. 1907).

233 Downs v. Swann, 73 A. 653, 654–55 (Md. 1909).

234 531 U.S. 32, 34–35, 42 (2000).

235 *Id.* at 34, 48.

236 *Id.* at 39–41.

237 Deterrence only works if the collection is open and notorious. *See* Skinner v. Ry. Lab. Exec. Ass'n, 489 U.S. 602, 630 (1989) (stating that a program "cannot serve as an effective deterrent unless violators know that they are likely to be discovered").

impaired employees with ease and perfect accuracy, the FRA regulations supply an effective means of deterring employees engaged in safety-sensitive tasks from using controlled substances or alcohol in the first place."[238] Similar logic has been applied to justify drug testing of students who engage in athletics,[239] the "airport screening program," which furthers an "obvious deterrent purpose,"[240] and collecting the DNA of convicted offenders, the theory being that if individuals know the government holds their DNA, it will tamp down on recidivism.[241]

Still, *Edmond* may doom current data collection efforts that are justified solely on the basis of having information available should it later prove useful in a criminal investigation.[242] Take the collection of ALPR data. It is indiscriminate. No person for whom information is collected is suspected of anything. It is done for no reason other than to have a hoard of information that might be useful for later criminal investigation.[243]

Commentators have questioned whether the *Edmond* Court's distinction between ordinary law enforcement and "special needs" is coherent and sustainable.[244] Even though *Edmond* prohibits searches without warrants if the "primary purpose" is ordinary law enforcement,[245] if there is another permissible purpose, the evidence still can

---

[238] *Id.* at 629.

[239] *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 661 (1995) ("Deterring drug use by our Nation's schoolchildren is at least as important as . . . deterring drug use by engineers and trainmen, which was the governmental concern in *Skinner*.").

[240] *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 675 n.3 (1989) (describing why the special needs program was upheld in United States v. Edwards, 498 F.2d 496 (2d Cir. 1974)).

[241] *See* Oscar Schwartz, *Do DNA Databases Make Would-Be Criminals Think Twice?*, UNDARK (Sept. 23, 2019), https://undark.org/2019/09/23/dna-database-deter-crime [https://perma.cc/J3BQ-SN77] (analyzing the strengths and weaknesses of the deterrence theory behind DNA databases).

[242] *See* ACLU v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015) (rejecting the "unprecedented and unwarranted" argument that collected information is *now* relevant if it *could be* relevant "at some unknown time in the future"); *cf.* Ams. for Prosperity Found. v. Bonta, 141 S. Ct. 2373, 2387 (2021) (holding that California cannot require disclosure of every charity's donors "just in case" it becomes relevant to an investigation).

[243] The government could claim that the mass collection of license plate data will serve to deter any crime. It's hard to see courts approving mass surveillance aimed at making sure the citizenry complies with every law on the books. This, after all, is totalitarianism. This same problem arises, albeit under a different guise, when the government purchases data *en masse*, such as the CLEAR database discussed *supra* Part I. Danielle Citron and I presently are working on a piece discussing how to deal with the situation of government acquiring information from third parties rather than collecting the information on its own.

[244] This scholarship is discussed in Part I of Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281 (2016), and in particular at pp. 307–10.

[245] City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000).

be used for pursuing charges against someone.[246] The problem is that it can be difficult to distinguish a case with a primary crime-fighting purpose from one in which the use of the criminal law was merely adjunct to the primary purpose.[247] After all, many of the individuals caught up in special needs searches, such as impaired drivers in *Sitz*, were headed right off to jail. Why was the primary purpose maintaining safe roads and not enforcing the law? Similarly, was the point of the drug checkpoint in *Edmond* to convict those carrying drugs or keep narcotics out of drug-ravaged neighborhoods? The Supreme Court has struggled with this problem itself.[248]

On the other hand, the *Edmond* principle seems deeply embedded in the law. Over and over in special needs cases, the Supreme Court has said that when the goal is discovering "evidence of criminal wrongdoing" warrants and probable cause are required.[249] *Edmond*'s reasoning also is reflected (as we saw) in the distinction between permissible and impermissible record-keeping requirements, as exemplified by *Marchetti*'s distinction from *Shapiro*.[250]

The correct answer may well be for *Edmond* to give way, but only so long as a regulatory scheme is in place that provides the necessary prerequisites. It is one thing to allow bulk data surveillance at the

---

246 *See, e.g.*, Merrett v. Moore, 58 F.3d 1547, 1550–51 (11th Cir. 1995) (approving of a suspicionless roadblock stop where police performed a license check and exposed cars to drug sniffing dogs because the state had at least one lawful purpose for the stop); United States v. McFayden, 865 F.2d 1306, 1312 (D.C. Cir. 1989) (allowing drug evidence from a suspicionless roadblock because the principal purpose was to allow police to check a driver's license and registration); Wrigley v. State, 546 S.E.2d 794, 797 (Ga. Ct. App. 2001) (finding that the stop's primary purpose was checking licenses and insurance cards with a secondary purpose of preventing drunk drivers).

247 *See, e.g.*, *Edmond*, 531 U.S. at 55–56 (Rehnquist, C.J., dissenting) (critiquing the primary purpose test given that identical activities could have multiple purposes); Jonathan Kravis, Case Comment, *A Better Interpretation of "Special Needs" Doctrine After* Edmond *and* Ferguson, 112 YALE L.J. 2591, 2595 (2003) ("[T]he distinction between law enforcement and non-law-enforcement purposes is not entirely clear.").

248 *See* Ferguson v. City of Charleston, 532 U.S. 67, 82–83 (2001) (rejecting a state hospital's policy of performing nonconsensual drug tests on pregnant women because even though the "ultimate goal" was to get the women into substance abuse treatment, the "immediate" goal was criminal evidence generation); *id.* at 86–87 (Kennedy, J., concurring) (disagreeing with the majority's distinction between "immediate" and "ultimate" law enforcement objectives in interpreting *Edmond*); *id.* at 99–100 (Scalia, J., dissenting) (rejecting the majority's logic of which goal was "immediate" and which was "ultimate").

249 *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995)) (rejecting the notion that the government may collect cell-site evidence simply because it might be pertinent to a criminal investigation; deeming it a "'gigantic' departure from the probable cause rule" which requires "some quantum of individualized suspicion" (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 560–61 (1976) (internal quotation marks omitted))).

250 *See supra* notes 132–40 and accompanying text.

whim of law enforcement agencies, with no clue as to why they do it, and no guardrails to restrain misuse. On the other hand, if a mass data collection scheme is approved legislatively, and if there are safeguards in place of the sort described below, then it is unclear whether courts are in a better position than the legislative body to judge the propriety of the reason for the collection.[251] Once again, this is a powerful argument for dooming surveillance without the appropriate prerequisites in place.

D. Efficacy and Relevance

Constitutional law isn't just about the giving of justifications; under typical "means-end scrutiny," courts usually evaluate whether a challenged program actually furthers its supposed justification. This is precisely what we saw courts do under the prerequisites analysis, though as was the case with justifications, the level of scrutiny can vary.[252] Sometimes judicial decisions talk in terms of whether the information sought is "relevant," or that there is a "reasonable relation," to the legislative purpose.[253] At other times they talk in terms of efficacy: Does the collection of the information factually further the government's purpose in having a collection program?[254]

Applying at least some level of scrutiny can be revealing, as it was in the Second Circuit's decision in *ACLU v. Clapper*. Congress had required that information collected by the NSA or other enforcement agencies be "relevant" to an "authorized investigation."[255] But "[r]elevance," the court pointed out, "does not exist in the abstract;

---

[251] *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208–09 (1946) ("It is not necessary, as in the case of a warrant, that a specific charge or complaint of violation of law be pending or that the order be made pursuant to one. It is enough that the investigation be for a lawfully authorized purpose, within the power of Congress . . . .").

[252] *See* Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1274 (2007) (comparing the tiers of review that courts employ when assessing the connection between challenged actions and the ends they are intended to promote).

[253] *See, e.g.*, State v. Williams, 761 S.E.2d 662, 668 (N.C. Ct. App. 2014) (holding that satellite monitoring of sex offenders "[is] rationally related to the purpose of protecting children and the more general public"); State v. Dykes, 744 S.E.2d 505 (S.C. 2013) (same); Perkey v. Dep't of Motor Vehicles, 721 P.2d 50, 53 (Cal. 1986) (finding that fingerprinting drivers' license applicants is "reasonably related" to the objective of intercepting applications from individuals that "pose a serious danger to public safety").

[254] *See, e.g.*, Heller v. District of Columbia, 801 F.3d 264, 277 (D.C. Cir. 2015) (finding "substantial evidence . . . that fingerprinting and photographing registrants will directly and materially advance public safety"); Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 183 (1st Cir. 1997) (finding that video surveillance of state employees "advance[d] the employer's legitimate, work-related interest in monitoring employee performance"); State v. Grady, 831 S.E.2d 542, 565, 567 (N.C. 2019) (citing a "lack of evidentiary support" for the notion that the satellite based monitoring program at issue was "effective at deterring crime" or "advance[d] its stated purpose of protecting the public from sex offenders").

[255] ACLU v. Clapper, 785 F.3d 787, 811 (2d Cir. 2015).

something is 'relevant' or not in relation to a particular subject."[256] That nexus failed in the case of NSA collection, because the "overwhelming" amount of the data being collected concerned "individuals who are not targets of an investigation or suspected of engaging in any crime whatsoever, and who are not even suspected of having any contacts with any such targets or suspects."[257]

The simple fact is that we have no clue about the efficacy or relevance of most surveillance data collection that is occurring today. That's because, in the absence of regulation, data is sucked up indiscriminately with no serious attempt even to state a purpose, let alone whether data collection will further that end. And that is unfortunate; some of this collection of surveillance data may be valuable, with the appropriate safeguards. To the extent it is not, we ought not to be collecting the data at all.

E. Safeguards

The prerequisites case law requires various safeguards, such as preventing misuse of information collected by the government and guarding the security of the data from public disclosure.[258] What safeguards are required varies with the nature of the collection itself. Because courts have not been asked to approve mass digital surveillance, the nature of the necessary safeguards around it are underdeveloped in the case law. Still, there is doctrine enough to understand the necessary contours.

The special needs case law sets out what is arguably the most important safeguard, which is that collection be regularized in a way that prevents the arbitrary exercise of discretion in collection by law enforcement officials.[259] Under Supreme Court doctrine, there must be "adequate substitutes" for the Fourth Amendment's probable

---

256 *Id.* at 815.

257 *Id.* at 814 n.7.

258 *See, e.g.*, United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (considering "potential for harm in . . . nonconsensual disclosure" and "adequacy of safeguards to prevent unauthorized disclosure" in determining whether collection of medical data was justified); Shelton v. Tucker, 364 U.S. 479 (1960) (striking down a statute compelling teachers to disclose organizational ties because the statute lacked safeguards, such as requiring the data be kept confidential); Ams. for Prosperity Found. v. Bonta, 141 S. Ct. 2373 (2021) (expressing doubt about safeguards in a California donor disclosure statute because data had been inadvertently released to the public during litigation).

259 *See* Delaware v. Prouse, 440 U.S. 648, 654–55 (1979) ("In those situations in which the balance of interests precludes insistence upon 'some quantum of individualized suspicion,' other safeguards are generally relied upon to assure that the individual's reasonable expectation of privacy is not 'subject to the discretion of the official in the field.'") (citations omitted).

cause and warrant process.[260] In ordinary investigations, probable cause prevents arbitrariness by narrowing down the target of government surveillance, and a warrant assures the probable cause determination is not made without neutral judicial supervision.[261] So the question becomes how to avoid this sort of arbitrariness when mass collection is at issue. In *Camara v. Municipal Court*, the Supreme Court approved administrative home inspections without classic probable cause but still required a novel sort of warrant, which ensured homes subject to inspection were chosen pursuant to a regularized plan that avoided the discretionary decisions of individual officers.[262] This was necessary, the Court said, "to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[263] Even when the Supreme Court permits warrantless searches of businesses, the question in these cases still is whether "the statute's inspection program, in terms of the certainty and regularity of its application, provides a constitutionally adequate substitute for a warrant."[264]

The best way to assure non-arbitrariness in the context of digital surveillance is universality. If data is being collected for some reason other than the existence of suspicion about a particular individual—say, deterrence—it is hard to justify subjecting some people to that surveillance and not others. *Delaware v. Prouse* is the key decision here. That case prohibited police from stopping motorists at will to check licenses and registration, precisely because of a concern for arbitrariness.[265] But stopping all motorists at a roadblock would be fine, the Court held, precisely because it avoids arbitrary (or discriminatory) selection.[266] One substitute for universality is true randomness: Justice Blackmun, concurring in *Prouse*, made the point that stopping every *nth* motorist also would suffice.[267] On the other hand, if the government is collecting personal information without individualized suspicion and in a way that neither is random nor universal, it

---

[260] *See* New York v. Burger, 482 U.S. 691, 703 (1987) (requiring that statutory safeguards "perform the two basic functions of a warrant," namely "advis[ing] . . . that the search is being made pursuant to the law and has a properly defined scope" and "limit[ing] the discretion of the inspecting officers").

[261] *See* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (discussing the role of the probable cause standard in safeguarding citizens from "unfounded charges of crime"); Camara v. Mun. Ct. of S.F., 387 U.S. 523, 532–33 (1967) (describing the protections provided by the warrant requirement).

[262] *Camara*, 387 U.S. 523.

[263] *Id.* at 528.

[264] Donovan v. Dewey, 452 U.S. 594, 603 (1981).

[265] Delaware v. Prouse, 440 U.S. 648 (1979).

[266] *Id.* at 663.

[267] *Id.* at 663–64 (Blackmun, J., concurring).

would seem a justification is in order for why some individuals are subjected to surveillance and not others.[268] For what it's worth, that's the view of the American Law Institute.[269]

Admittedly, the universality requirement may seem to bump into the prerequisite of establishing the relevance of information—but not necessarily, and indeed just the opposite might be true. At first blush, the more information that is collected, the less germane it would seem to be to any particular need. That is what the *Clapper* court was alluding to. But if information of a particular type is collected for later investigative purposes, it makes sense to have the widest pool of information so that the investigation will locate the culprit. If, for example, the telephone metadata at issue in *Clapper* was useful in fighting terrorism, why not have the widest pool of such metadata? Of course, this sort of widespread collection is invasive—but that is exactly why prerequisites such as authorization are essential, to ensure society really intends to go down this road. What the *Clapper* court held, as we have seen, is that such authorization was lacking. In truth, widespread collection assures the burdens fall widely as well, bolstering the effectiveness of the political process. (Even if such collection is authorized, courts still can review the collection under constitutional guarantees such as the Fourth Amendment.)

Minimization seems another clear safeguard, which is to say the government should not collect and keep more than it needs to achieve the stated justification for collection. This is what the ban on "fishing expeditions" around subpoenas, discussed in Part II, was all about.[270] It also was the case in the *Nixon* decision, in which the Court explained that "the Act provides procedures and orders the promulgation of regulations expressly for the purpose of minimizing intrusion into appellant's private and personal materials."[271] Similarly, in *Berger v. New York*, the Supreme Court struck down New York's wiretapping regime, on the ground that although wiretapping might be acceptable if it were "precise and discriminate," what the New York law permitted was "indiscriminate."[272] Congress responded by passing the federal wiretap act, which not only requires precision in targeting electronic surveillance, but also contains numerous other safeguards,

---

[268] *See* Friedman & Stein, *supra* note 244, at 320–23 (arguing that in the absence of probable cause or generality, clear justification for dragnet surveillance of groups is necessary to avoid arbitrary and discriminatory policing).

[269] *See* PRINCIPLES OF THE L.: POLICING § 5.04 (AM. L. INST., Tentative Draft No. 3, 2021); *id.* § 5.05.

[270] *See supra* notes 117–26 and accompanying text.

[271] Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 462 (1977).

[272] 388 U.S. 41, 58 (1967).

such as minimizing the collection of irrelevant information and that of people who are not targets of investigation.[273]

Then there are the requirements of data security. In Nixon's challenge to the review of his papers, the Court pointed to the fact that the screening would take place by archivists with "an unblemished record for discretion."[274] In *Whalen*, the Supreme Court described in elaborate detail the rules regarding data security and disclosure.[275] The prescription records were stored physically in a vault, the electronic records were kept on tape in a locked closet, and the data only could be accessed "off-line," meaning no terminal other than that in the computer room could access the data.[276] A very limited number of employees had access to the data. And anyone who willfully released the information publicly was subject to criminal penalties.[277] My suspicion is that much law enforcement surveillance data falls quite short by *Whalen*'s standards. If the government is to be allowed to collect all this data, mandating data security would seem an essential prerequisite.

Although much of our attention has been on collection, one of the more intriguing questions is what sort of predicate government should have to have to access data that it previously has collected. The question may seem odd: If the government has the data, can't it use it? But that is putting a lot of power in the hands of government—and individual officers—to go trolling through the data for whatever reason. As the contending *Carpenter* opinions underscore, when government seeks access to data in private hands, there's tension between providing protections against government snooping and the fact that if a warrant and probable cause were required for each database search, investigations might never get off the ground.[278] This tension is even more acute when the government possesses a deep pool of information about us. Can the government scoop up everything it desires about each of us, and then down the road decide to aggregate it and use it in any way the authorities wish? Today, individual police department policies may specify when particular data they possess may be

---

[273] *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2518(4) (requiring that interception of electronic communication be specific as to the person whose communication is to be intercepted, describe the offense the communication relates to, and the time period in which the interception is authorized); § 2518(5) (requiring that order must direct interception to be conducted in such a way that minimizes the interception of non-pertinent communications).

[274] *Nixon*, 433 U.S. at 462.

[275] Whalen v. Roe, 429 U.S. 589 (1977).

[276] *Id.* at 594.

[277] *Id.* at 595.

[278] Carpenter v. United States, 138 S. Ct. 2206 (2018).

accessed, but even where those predicates exist, they tend to be quite general, allowing access for any "legitimate law enforcement purpose."[279] And there typically is little in the way of sanction for abuse. It's incongruous and troubling that government would face limitations on access to data when it is held in private hands but can sidestep predicate issues simply by being the depository of the data.

Congress's resolution of the dispute over NSA collection of telephone metadata may provide a solution to this problem. The NSA was collecting vast amounts of data indiscriminately, which when discovered led to widespread and understandable public concern. Congress ultimately concluded the solution was to insist the data remain in third-party hands and impose a predicate for government access.[280] Pursuant to the USA FREEDOM Act, the telephone data would remain with the providers, and government entities would need a court order to access it, based on "reasonable suspicion."[281]

Perhaps, then, even if government collection of data is permissible, the government never should be allowed to hold the data, and some sort of predicate for access always should be required for government to access it. Alternatively, the government might be allowed to hold the data, but in a secure and auditable way, and access could be permitted only upon court order. Predicates could vary—from the lowest, such as relevant to an ongoing investigation, to the more traditional probable cause—depending on the nature and quantity of the information being accessed.

F. Process and Judicial Review

The final element that any constitutional information-gathering scheme must contain is the opportunity for judicial review. The forms taken by judicial review, as well as the timing, vary widely from program to program. For example, subpoenas can be challenged before there is compliance.[282] Statutory schemes, like those involved in required records, can be challenged ex ante in lieu of compliance, but

---

[279] *See, e.g.*, Commonwealth v. McCarthy, 142 N.E.3d 1090, 1096 n.4 (Mass. 2020) (describing the Massachusetts policy stipulating that ALPR databases may be accessed by police officers "only for official and legitimate law enforcement purpose").

[280] USA FREEDOM Act of 2015, H.R. 2048, Pub. L. 114–23.

[281] *See* Forsyth, *supra* note 90, at 1338–39 ("If the government can demonstrate a reasonable, articulable suspicion that a specific selection term is associated with a foreign power . . . the FISC may issue an order for the ongoing, daily production of call detail records held by telephone companies.").

[282] *See, e.g.*, Fed. Election Comm'n v. Larouche Campaign, 817 F.2d 233, 233–34 (2d Cir. 1987) (reviewing challenge to an FEC subpoena before campaign's compliance); Loc. 1814, Int'l Longshoremen's Ass'n, AFL-CIO v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267, 269 (2d Cir. 1981) (modifying Commission subpoena before compliance).

they also can be challenged at the moment that the government wishes to use evidence so obtained.[283] Challenges can be brought individual-by-individual, or—as in the *Whalen* case—in the aggregate, either by a formal class or by a group of affected individuals.[284]

That judicial review should be available is hardly surprising. The general presumption is that absent clear preclusive statutory language, judicial review is appropriate.[285] When constitutional rights are at stake, it may be required.[286]

As we have already seen, for most policing data collection, there is no authorization, and thus not a provision for judicial review, outside the usual Fourth Amendment route. Moreover, when surveillance programs are secret, there is no one on notice to challenge them anyway. And, agencies often engage in the practice of "parallel construction," which is to say that in criminal cases they obscure the initial basis for investigation so as to keep certain intelligence-gathering tools secret.[287]

Maintaining a system of surveillance data collection on countless individuals, most of whom are suspected of nothing, without an orderly way to challenge that collection, is untenable. It is the antithesis of the rule of law.

---

[283] *See supra* note 140.

[284] *See, e.g.*, *In re* Grand Jury Proceedings, 776 F.2d 1099, 1100 (2d Cir. 1985) (concerning individual subpoena challenge by grand jury witness); Whalen v. Roe, 429 U.S. 589, 595 (1977) (concerning aggregate challenge by group of affected individuals, including affected patients, doctors, and two physician associations); Paul P. v. Verniero, 170 F.3d 396, 398 (3d Cir. 1999) (concerning aggregate class action challenge).

[285] *See* Dep't of Com. v. New York, 139 S. Ct. 2551, 2567 (2019) ("The Administrative Procedure Act embodies a 'basic presumption of judicial review' . . . [except if] a relevant statute precludes it.") (quoting Abbott Laboratories v. Gardner, 387 U.S. 136, 140 (1967), and citing 5 U.S.C. § 701(a)(1)).

[286] *See* Webster v. Doe, 486 U.S. 592, 603–04 (1988) (finding congressional preclusion of judicial review of a claim of constitutional rights infringement would pose a "serious constitutional question"). *Compare* State v. Dykes, 744 S.E.2d 505, 510 (S.C. 2013) (holding unconstitutional a statute mandating lifetime satellite monitoring of convicted sex offenders because it precluded "any opportunity for judicial review to assess a risk of reoffending"), *with* North Carolina v. Williams, 761 S.E.2d 662, 667 (N.C. Ct. App. 2014) (upholding a similar statutory scheme that provided for "a determination of dangerousness prior to imposing enrollment in a satellite-based monitoring program *and* the possibility for review for later termination").

[287] Trevor Aaronson, *Welcome to Law Enforcement's "Dark Side": Secret Evidence, Illegal Searches, and Dubious Traffic Stops*, THE INTERCEPT (Jan. 9, 2018), https://theintercept.com/2018/01/09/dark-side-fbi-dea-illegal-searches-secret-evidence [https://perma.cc/UX7D-TPLF].

IV
How the Constitution Applies to Surveillance Data Collection

So far, we've seen that when the government collects or uses personal information, and that collection or use is challenged, courts regularly require a set of constitutional prerequisites. Beginning with the most basic one, that of statutory authorization, there is a notable uniformity to these prerequisites. This is true no matter the sort of information, or under which clause of the Constitution the challenge arises. We've also seen how those prerequisites would apply to mass surveillance digital data collection.

In order to permit courts to require the prerequisites, though, what the government does must implicate the Constitution. That's what gives courts their authority over data collection and use. This Part identifies a number of constitutional doctrinal avenues available to courts, allowing them to impose the prerequisites on government collection and use of surveillance data.[288]

It is theoretically possible, of course, that absent constitutional action by courts, legislative bodies would enact these statutory prerequisites on their own. But they have not done so, largely—one surmises—due to the set of political considerations identified in Part II. An advantage of judicial review is that it is likely to break the public choice logjam that has kept legislatures from acting. Law enforcement agencies—police and prosecutors—are good at stymying legislation.[289] But they are equally good at motivating legislation when they want it.[290] At present, the default of no legislation works in the favor of law enforcement agencies, who do not want that sort of regulation. But once a court rules the government is prohibited from utilizing surveillance absent regulation, law enforcement agencies are likely to motivate legislative bodies to act. Then the question becomes the quality of the legislation; as the sources cited below suggest, there is

---

[288] That's just the federal Constitution—as we will see in passing, state constitutions often diverge from the Supreme Court's narrow interpretations, providing yet more entryways to judicial action.

[289] *See supra* notes 89–90 and accompanying text. *See also* Luke Broadwater & Catie Edmonson, *Police Groups Wield Strong Influence in Congress, Resisting the Strictest Reforms*, N.Y. Times (Mar. 8, 2021), https://www.nytimes.com/2020/06/25/us/politics/police-reforms-congress.html [https://perma.cc/C226-KM3E].

[290] *See* Kevin M. Keenan & Samuel Walker, *An Impediment to Police Accountability—An Analysis of Statutory Law Enforcement Officers' Bills of Rights*, 14 B.U. Pub. Int. L.J. 185 (2005) (discussing adoption of statutory bars to police accountability).

some room for hope there, but it also is the case that the Constitution requires that at a minimum all the prerequisites be met.[291]

A. The Implausible Absence of the Constitution

Let's start with a little common sense; put your doctrinal hat aside for a moment and think about what's at stake from a policy perspective. If the doctrinal discussion that follows is off the mark in its entirety, it means that the Constitution continues to apply *not at all* to what ultimately will prove one of the greatest grabs by the government of personal data in history, one that can and will happen in racially (and other) discriminatory ways, and with all the harms set out in Part I. Absent constitutional coverage, or the statutes that as we have seen are not getting adopted, the government would be free to "keep a comprehensive, permanent, searchable digital record of every person or entity with whom" we all "have ever exchanged a phone call, email, text message, or for that matter physical letter."[292] It also could hold all our social media posts, financial transactions, health information, websites visited, and information from our smart devices.[293] Not only that, but it could aggregate all that information in the ways it chooses, learning whatever the composite reveals. The information could be collected, retained, and manipulated, in the "unbridled discretion" of "executive and administrative officers," including in ways that have disparate impacts on individual groups, especially Black and brown individuals, vulnerable individuals, and marginalized individuals.[294] The government could release all this information publicly in any way and at any time it chose. All that would stand between this and our liberty is the occasional "narrow" decision from the Supreme Court ruling one or another collection in

---

[291] It's entirely fair to have concerns about precisely what legislation will emerge. But almost anything would be better than the laissez-faire situation today. Instances in which legislative bodies have acted to authorize and regulate surveillance give some basis for hoping that once there is open public debate, there will be a reasonable accommodation of law enforcement and individual security interests. *See, e.g.*, TENN. CODE ANN. § 55-10-302(b) (West 2014) (limiting retention of license plate reads to 90 days); N.H. REV. STAT. ANN. § 261:75-b(VIII) (2016) (limiting retention of license plate reads to 3 minutes); CAL. PENAL CODE § 1546.1(g) (West 2017) (limiting retention of data voluntarily provided by internet service providers to 90 days); VA. CODE ANN. § 19.2-60.1(B)–(C) (West 2019) (requiring a warrant for the use of drones, with exceptions for exigent circumstances); N.H. REV. STAT. ANN. §§ 651-F:1–8 (2010) (carefully regulating state fusion center). Besides—and this is crucially important—once a regulatory scheme is in place, it will be easier for courts to measure that scheme against constitutional norms.

[292] Brazeal, *supra* note 26, at 1017.

[293] *Id.* at 1017–19.

[294] Marshall v. Barlow's, Inc., 436 U.S. 307, 323 (1978). *See supra* notes 58–61 on how data collection is raced and classed.

or out of bounds. We have seen how well that works in a world of rapidly advancing technology.

No wonder judges have begun to get queasy, even in the area of individual data collection. Even the dissenting Justices in *Carpenter* hardly were sanguine about the threats to personal security of overweening surveillance.[295] The Massachusetts Supreme Judicial Court has concluded that just one real-time ping of a person's cell phone to locate the person is unconstitutional.[296] As the concurrence pointed out, "To know that the government can find you anywhere, at any time is—in a word—'creepy'": It "places the liberty of every [person] in the hands of every petty officer."[297] Upholding the use of ALPRs in one case, the Massachusetts court still expressed concern that "new technologies" "give police surveillance powers akin to . . . general warrants."[298] "Resource constraints aside, we imagine Massachusetts residents would object were the police continuously to track every person's public movements by traditional surveillance methods, absent any suspicion at all."[299] The South Dakota Supreme Court balked at the long-term use of pole cameras, something the *Carpenter* Court seemed at pains to protect, given that those cameras permit the police to see "the aggregate of all of [the defendant's] coming and going from the home, all of his visitors, all of his cars, all of their cars, and all of the types of packages or bags he carried and when."[300]

These tentative moves to reel in the use of surveillance technologies are entirely consistent with the fact that constitutional interpretations necessarily evolve to meet new circumstances.[301] This isn't a "living Constitution" argument: Plenty of judges have recognized that how we understand the Constitution necessarily has to change as tech-

---

[295] *See* Carpenter v. United States, 138 S. Ct. 2206, 2246–47 (2018) (Alito, J., dissenting) ("I share the Court's concern about the effect of new technology on personal privacy . . . ."); *id.* at 2262 (Gorsuch, J., dissenting) (asking "[w]hat's left of the Fourth Amendment?" under existing doctrine and offering a positive law alternative as more rights-protective).

[296] Commonwealth v. Almonor, 120 N.E.3d 1183 (Mass. 2019).

[297] *Id.* at 1201–02 (Lenk, J., concurring) (quoting United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting) and Commonwealth v. Blood, 507 N.E.2d 1029, 1035 (Mass. 1987)).

[298] Commonwealth v. McCarthy, 142 N.E.3d 1090, 1099 (Mass. 2020).

[299] *Id.* at 1099.

[300] State v. Jones, 903 N.W.2d 101, 111 (S.D. 2017) (quoting United States v. Garcia-Gonzalez, No. 14-10296, 2015 WL 5145537, at *5 (D. Mass. Sept. 1, 2015)).

[301] *See* Lawrence Lessig, *Translating Federalism:* United States v. Lopez, 1995 SUP. CT. REV. 125, 132 (1995) (arguing that the scope of constitutional powers and protections "turn upon facts in the world, and as these facts change, the scope of the power too is seen to change" requiring courts to adapt the original structure of the Constitution "to neutralize the effects of these changes in the world").

nology shifts around it.[302] Even originalist judges. One of the most insistent voices on this very point was Antonin Scalia. "It would be foolish," he wrote in *Kyllo v. United States*, "to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[303] *Foolish*. *Kyllo* held that using a thermal heat sensor, with no physical trespass whatsoever, to discover the use of "grow" lamps signaling marijuana cultivation was a "search" that required a warrant. This was necessary, Justice Scalia explained, in a phrase that has become a tagline for recent search decisions, to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[304]

And evolve is precisely what interpretations of the Constitution have done—a point that bears keeping in mind as one considers the doctrinal arguments that follow. In *Olmstead v. United States*, the Supreme Court held wiretapping entirely outside the Constitution, and there it stood until the Court reversed itself in *Berger v. New York* and *Katz v. United States*.[305] Is that so surprising? Is it even imaginable that today the government would be able to wiretap us at will? So why collect all our other personal data? The same thing happened in *Jones v. United States*, which held that tracking a car via a GPS device was a "search"—despite decisions like *Knotts* and *Karo* that previously had held tracking cars on public roads was not a search.[306] Similarly, for decades it was thought that all that was required for subpoenas was to meet the "reasonable" language of the Fourth Amendment in the way described in Part II—until *Carpenter* held that for particularly invasive subpoenas, warrants and probable cause were required as well.[307] In short: What implicates the Constitution necessarily changes to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[308]

---

[302] *See, e.g.*, United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations.").

[303] Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

[304] *Id.* at 34.

[305] Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Berger v. New York, 388 U.S. 41 (1967), *and* Katz v. United States, 389 U.S. 347 (1967).

[306] *Jones*, 565 U.S. 400; United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

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

[308] *Kyllo*, 535 U.S. at 34; *accord Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting) (citing *Kyllo*, 535 U.S. at 40) ("Nor does this mean protecting only the specific rights known at the founding; it means protecting their modern analogues too.").

The Justices have felt compelled to move slowly around surveillance technologies. As the Chief Justice put it in *Carpenter*, "when considering new innovations" the Justices must "tread carefully" lest they "embarrass the future."[309] We saw the reasons for this in Part I. Under existing doctrine, the implication of deeming something a search is that a warrant and probable cause are required.[310] Yet, as Justices Kennedy and Alito argued at length in *Carpenter*, that would stop most investigations before they started.[311] And when a ruling is placed on constitutional grounds, that bars a legislature from changing the rule. That's concerning to the Justices, who often have no clue about the efficacy of these tools and are reluctant to jeopardize public safety.[312] Trapped in that constitutional box, judges understandably balk.

But here is the point to which I keep returning: *If courts adopt the prerequisites approach, none of these concerns remain*. Judges don't need to rule anything out of constitutional bounds. They simply can insist on democratic decisionmaking about what sort of surveillance is appropriate, including some very reasonable safeguards, especially when the government is surveilling in bulk a population of individuals who are not suspected of any offense. They can reserve on the constitutional propriety of collection until they see what regulation is adopted.

To require prerequisites, the Justices need only find a way to conclude that the Constitution applies at all to mass digital data collection. It should not be that difficult to hold that the Constitution says *something* about such overweening surveillance. The following discussion offers several alternatives. The most plausible (in my view) are special needs searches or information privacy rights, but readers may prefer another choice. As Part II made clear, the Supreme Court has relied on a wealth of constitutional provisions to require prerequisites around personal data collection.

---

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

310 *See Katz*, 389 U.S. at 357 ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . .").

311 *See, e.g.*, *Carpenter*, 138 S. Ct. at 2233–34 (Kennedy, J., dissenting) ("[T]he Court's holding . . . limits the effectiveness of an important investigative tool for solving serious crimes. . . . These records often are indispensable at the initial stages of investigations . . . ."); *id*. at 2256 (Alito, J., dissenting) (warning that "[m]any investigations will sputter out at the start, and a host of criminals will be able to evade law enforcement's reach").

312 *See supra* notes 98–101 and accompanying text.

B. The Fourth Amendment

1. It's a Special Needs Search

Deeming digital surveillance a "search" within the meaning of the Fourth Amendment is the most logical way to bring surveillance under control. The special needs doctrine, or an analogy to it, is the way to go. Properly applied, the special needs doctrine aligns quite closely with the prerequisites approach.

The critical point, once again, is that concluding something is a "search" implicating the Fourth Amendment does not necessarily require a warrant, or probable cause, or any cause for that matter. As long ago as *Oklahoma Press Publishing Co. v. Walling*, the Court deemed subpoenas "figurative" or "constructive" searches.[313] Unlike the battering of doors, and the physicality of exploring bodies, subpoenas demand (only) that the target produce the identified papers or other information. They still are "searches" that must be "reasonable," but they don't require warrants or probable cause.[314] As Justice Alito wrote, dissenting in *Carpenter*, "[w]e now evaluate subpoenas *duces tecum* and other forms of compulsory document production under the Fourth Amendment, although we employ a reasonableness standard that is less demanding than the requirements for a warrant."[315]

The same is true of special needs searches. Although some require cause when the search is aimed at a specific individual, e.g., the search of a student's bag, most do not.[316] That's precisely because they are programmatic, aimed at a wider population, so requiring cause makes no sense. Even though cause is not required, however, meeting the prerequisites, including an "adequate safeguard" for the lack of a warrant or probable cause, is.[317]

There are three seeming difficulties in applying the special needs doctrine to mass digital surveillance, but all are utterly surmountable. First, as we saw in Part II, the special needs doctrine does not align perfectly with the prerequisites at present. Instead, the Court relies on a fuzzy balancing test. But as we also saw in *Skinner*, properly applied,

---

313 Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 202 (1946).

314 *See supra* notes 113–14 and accompanying text (describing this approach of *Hale v. Henkel*).

315 *Carpenter*, 138 S. Ct. at 2252 (Alito, J., dissenting).

316 *See* United States v. Martinez-Fuerte, 428 U.S. 543, 560–61 (1976) ("[S]ome quantum of individualized suspicion is usually a prerequisite to a constitutional search or seizure. But the Fourth Amendment imposes no irreducible requirement of such suspicion.").

317 *See supra* notes 193–204 and accompanying text (discussing special needs searches in context of information collection).

that balancing test ticks off all the prerequisites quite well.[318] Given how hard the balancing test has proven to apply—about which commentators have been derisive[319]—the Justices would do well to clean up their special needs act more generally, and the prerequisites approach is precisely how to do it.

Second, to the extent mass digital surveillance is for purposes of ordinary law enforcement, the *Edmond* doctrine—which bars programmatic searching for just such purposes—seems a problem. But, as I argued in Part III, the solution to this is simply to refine *Edmond* itself. Although there is a strict bar on using surveillance data for criminal investigative purposes when it is done at the whim of law enforcement officials, the bar might be loosened to the extent such data is collected in accord with the six statutory prerequisites. (Otherwise, for what it is worth, any programmatic mass data collection that constitutes a search is going to be flat-out unconstitutional).

Third, one might argue that much data collection is not a "search" at all within the meaning of the Fourth Amendment—but here the subpoena cases offer the answer. As discussed above, courts have shied away from deeming a surveillance a search because of the consequences. For example, does it make any sense to require warrants for mass data collection? However, as discussed at the very beginning of Part II, courts confronted precisely this issue around subpoenas and solved it. Given that subpoenas involved no breaking of doors, no entry into residences or offices, they were deemed "figurative" or "constructive" searches, for which no warrant was required, but the prerequisites were.[320] As the Supreme Court said in *Oklahoma Press Publishing Co. v. Walling*, "[t]he requirement of 'probable cause . . .' . . . is satisfied . . . by the court's determination that the investigation is authorized by Congress, is for a purpose

---

[318] *See supra* notes 194–201 (discussing how the *Skinner* decision touches on the six prerequisites).

[319] *See* Friedman & Stein, *supra* note 244, at 297–300 (critiquing courts' ability to assess either side of the special needs balance); Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 106–07 (1991) (criticizing the Court's willingness to "exaggerate the state's interests . . . and to trivialize the individual's interests"); Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 352–54 (2009) (presenting survey evidence casting doubt on courts' ability to effectively distinguish a minimal government intrusion into individual privacy from a serious one).

[320] Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 202, 209 (1946); *accord* CHRISTOPHER SLOBOGIN, VIRTUAL SEARCHES: REGULATING THE COVERT WORLD OF TECHNOLOGICAL POLICING (forthcoming Oct. 2022) (manuscript at 149) ("The data collection phase of [the NSA's Total Information Awareness program] and its progeny . . . is the classic example of a program-driven virtual search."). *See generally supra* notes 112–27 and accompanying text (discussing the subpoena prerequisites).

Congress can order, and the documents sought are relevant to th[at] inquiry."[321] The Court may well have to figure out on a case-by-case basis which surveillance techniques are sufficiently invasive as to require the prerequisites be met. Some (such as ALPRs or DNA collection) may cross the line; others may not. But, to quote the *Carpenter* Court, many of the digital technologies record our "physical location and movements"—indeed our "past movements"—in a way humans never could.[322] Others provide an "intimate window" into our lives and "associations."[323] Still others capture the "modern-day equivalents" of our "papers" and "effects."[324] Surely much of today's mass data collection is just the sort of "too permeating police surveillance" to which the Justices say the Fourth Amendment applies.[325] It simply is not too much to ask that legislative bodies approve and regulate these technologies if they are to be used at all. Indeed, it's hard to see how we "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" without legislative prerequisites in place, including necessary safeguards.[326]

2. *It's a Seizure*

But if not a search, why is not the bulk collection of surveillance data a Fourth Amendment "seizure?" Christopher Slobogin points out that the collection of surveillance data is actually "in effect, closer to a seizure than a search."[327] The government, as he explains it, is "engaged in seizing and recording evidence with an aim to enabling subsequent searches."[328] There's actually precedent for deeming the collection of surveillance data a seizure, though it seems—on this point at least—to have slipped by unnoticed by most courts and commentators. In *ACLU v. Clapper*, plaintiffs claimed the NSA's bulk collection of telephone metadata was an unconstitutional search.[329] The Second Circuit concluded, however: "[S]uch collection is more appropriately challenged . . . as a seizure rather than a search."[330]

---

321 *Okla. Press*, 327 U.S. at 209.

322 Carpenter v. United States, 138 S. Ct. 2206, 2215–16 (2018).

323 *Id.*

324 *Id.* at 2217, 2222 (citing *id.* at 2230 (Kennedy, J., dissenting)).

325 *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

326 *Id.* (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

327 SLOBOGIN, *supra* note 320 (manuscript at 150); *accord* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN L. REV. 285, 327 (2015) (distinguishing "seizure" of data, and latter "search" of it to perform analysis).

328 SLOBOGIN, *supra* note 320.

329 ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

330 *Id.* at 801.

In the spirit of full disclosure, the words elided by the ellipses above state "at least from a standing perspective."[331] Ultimately, as we have seen, the court struck down the data collection at issue as unauthorized by Congress.[332] But a threshold question in the case was whether the plaintiffs had standing even to raise the question. They argued standing existed, because the collection was a "search." Reluctant to wade into that tricky issue, the court simply deemed the collection a seizure.[333] The Second Circuit's conclusion that the collection of personal data is a seizure sufficient to invoke Fourth Amendment standing has been followed by courts.[334]

Why, and on what logic, should government conduct constitute a seizure for standing purposes, and not for the merits? The standing test requires an "actual" injury traceable to the government, which could be redressed by a court ruling.[335] I can't think of another area of law in which the injury that grants a plaintiff standing does not serve also to call for constitutional analysis on the merits.

Justices Thomas and Gorsuch seemed to be getting at this point in *Carpenter*, although they did not say it this precise way. Expressing great skepticism about the workability of the *Katz* test, Justice Gorsuch urged a return to the "traditional approach" that "asked if a house, paper or effect was *yours* under the law."[336] Justice Thomas's critique of *Katz* sounded similarly; under his view the point of the Fourth Amendment was to "secure" one's "property"—such that to prevail Carpenter had to show the government had taken something that was "*his*."[337] Although framed in the "search" terms of the

---

331 *Id.*

332 *See supra* note 226.

333 *See Clapper*, 785 F.3d at 801–02.

334 *See, e.g.*, Amidax Trading Grp. v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d Cir. 2011) (government's collection of an individual's financial records from service that routes financial transactions is sufficient injury to confer standing under the Fourth Amendment); Janfeshan v. U.S. Customs & Border Prot., No. 16-CV-6915, 2017 U.S. Dist. LEXIS 151058, at *19 (E.D.N.Y. Aug. 18, 2017) (plaintiff had standing under the Fourth Amendment "stemming from the copying and retention of the digital contents of his phone").

335 Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010) ("Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.").

336 Carpenter v. United States, 138 S. Ct. 2206, 2267–68 (2018) (Gorsuch, J., dissenting).

337 Justice Thomas didn't feel that the Telecommunications Act established that ownership interest, *see id.* at 2239–42 (Thomas, J., dissenting), whereas Justice Gorsuch was unsure on the record, *see id.* at 2272 (Gorsuch, J., dissenting).

majority, these descriptions seem to be much more about the sort of grabbing of personalty that we better associate with seizures.[338]

If the collection of surveillance data is in fact a seizure, then the requirement that it not be "unreasonable" once again implicates the prerequisites. Most seizures, of course, require probable cause, if not warrants. But as we saw in the special needs and subpoena cases alike, requiring probable cause for programmatic searches makes no sense. Thus, once again, the answer is to substitute the prerequisites for those more common Fourth Amendment protections.

C. The Due Process Clause

If the arguments about the Fourth Amendment do not persuade, the Due Process Clauses of the Fifth and Fourteenth Amendments afford three alternative bases for requiring prerequisites before the government conducts surveillance on us: liberty, property, and privacy.

1. The Opening for Due Process

The Supreme Court has a rule that superficially at least would suggest we should focus on the Fourth Amendment, not the Due Process Clause. The rule goes like this: If two constitutional clauses (or more) appear to govern a plaintiff's constitutional complaint, courts should analyze the claim under the clause that applies most specifically to that circumstance.[339] Thus, for example, claims of exces-

---

[338] Indeed, some intellectual property scholars have suggested we should consider whether people have property interests in their personal data, with consequences for those who then take, or seize, it. *See, e.g.*, Sylvie Delacroix & Neil D. Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIV. L. 236 (2019) (advocating for the creation of a property right in personal data and the establishment of "data Trusts" to help manage and oversee the exercise of these rights); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1196 (2016) (arguing that data, when collected and stored in bulk, might be considered a commodity). Michael Pollack even has argued forthrightly that something like a Takings Clause analysis (legislatively adopted) should apply to government grabs of personal data like those we are discussing. Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77 (2019). To be sure, other commentators offer normative arguments against creating rights in our data as against private companies commodifying it. *See* Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1138 (2000) (raising concerns about the alienability of personal information); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1303 (2000) (same); Christine Rinik, *Data Trusts: More Data than Trust? The Perspective of the Data Subject in the Face of a Growing Problem*, 34 INT'L REV. L., COMPUTS. & TECH. 342, 348–49 (2019) (discussing the difficulties of obtaining consent for personal data collection and exploitation). But none of their arguments against private commodification apply when the entity grabbing our data is the government.

[339] *See, e.g.*, Medina v. California, 505 U.S. 437, 443–44 (1992) (limiting use of Due Process Clause in favor of specific guarantees in Bill of Rights in criminal cases).

sive force in the course of an investigatory stop or arrest are to be analyzed under the Fourth Amendment, not the Due Process Clause. "Because the Fourth Amendment provides an explicit textual source of constitutional protection against this sort of physically intrusive governmental conduct, that Amendment, not the more generalized notion of 'substantive due process,' must be the guide for analyzing these claims."[340] Sometimes this matters in that judicial decisions arising under the Due Process Clause may provide greater protection to claimants than the protections afforded by the Fourth Amendment.[341]

But if government surveillance is neither a "search" nor a "seizure," then this constitutional traffic direction rule actually favors the Due Process Clause. That's because if government conduct is neither a search nor a seizure, the Fourth Amendment effectively does not apply *at all*.[342] It is not that it fails to afford relief, which was the situation with the excessive force cases; rather, it simply is inapplicable. There is not, in the Court's own formulation, "an explicit textual source of constitutional protection against" the governmental conduct of which the claimant complains.[343] And so the door is open to turning to the Due Process Clause.

2. Liberty and Property

The Due Process Clause prohibits depriving people of life, liberty, or property without appropriate legal protections. Just as "search" and "seizure" guard the door of the Fourth Amendment, words like "liberty" and "property" are the thresholds one must cross to gain protection under the Due Process Clause.

We've already seen the beginnings of an argument for deeming the collection of personal data "property." That is the direction Justices Gorsuch and Thomas were headed in *Carpenter*, albeit under the Fourth Amendment. They were saying that in some instances, positive law might create property interests in data. And that is the con-

---

[340] Graham v. Connor, 490 U.S. 386, 395 (1989); *see also* Albright v. Oliver, 510 U.S. 266, 273 (1994) (holding that because the Fourth Amendment provided explicit textual source, the Fourth Amendment, and not substantive due process, would be used to assess plaintiff's claims).

[341] *See generally* Pamela R. Metzger & Janet C. Hoeffel, *Criminal (Dis)Appearance*, 88 GEO. WASH. L. REV. 392 (2020) (discussing this phenomenon in the Court's decisions).

[342] *See, e.g.*, United States v. Attson, 900 F.2d 1427, 1429 (9th Cir. 1990) ("[T]he [F]ourth [A]mendment will only apply to governmental conduct that can reasonably be characterized as a 'search' or a 'seizure.'").

[343] *Graham*, 490 U.S. at 395.

clusion of commentators who favor allowing us to commodify our data.[344]

There's a similar basis in case law for deeming the collection of some amount of surveillance data a deprivation of "liberty." In *Grady v. North Carolina*, the Supreme Court held forcing someone to wear a location tracking device as part of supervised release constituted a "search" for Fourth Amendment purposes.[345] But other courts, particularly in the civil context (e.g., a law that requires monitoring of sex offenders despite having served one's sentence), have deemed such monitoring to constitute a deprivation of liberty sufficient to invoke Due Process concerns. For instance, in *State v. Dykes* the South Carolina Supreme Court determined that satellite-based monitoring programs implicated "a protected liberty interest to be free from permanent, unwarranted governmental interference" and thus warranted "minimal due process protection."[346] As a result, the court looked to the familiar requisites: that the monitoring program have statutory authorization, a rational basis, and be non-arbitrary in its application.[347]

3. Privacy

Perhaps the precedential approach most on point, though, is the right to informational privacy identified in *Whalen v. Roe*. *Whalen* was the challenge to the collection of information about prescriptions of controlled substances.[348] Although the plaintiff ultimately lost on the merits, the Court was unanimous in holding that the Constitution protected the "disclosure of personal matters."[349] The extent and nature of information being collected by the government surveillance data programs far exceed what was at issue in *Whalen*.

Is *Whalen* still good law? It has been invoked in many cases, yet the Supreme Court in 2011 wrote that it merely "assume[d], without deciding" that the Constitution protects a privacy right of the sort articulated by *Whalen*.[350] But as I argued above, even if privacy rights are under attack in some ways, those attacks have not extended to informational privacy.[351] Numerous cases have relied on *Whalen*'s

344 *See supra* note 338 and accompanying text.

345 575 U.S. 306 (2015).

346 744 S.E.2d 505, 509 (S.C. 2013).

347 *Id.* at 507; *see also, e.g.*, Paul P. v. Verniero, 170 F.3d 396, 400–01 (3d Cir. 1999) (engaging in similar analysis); Doe v. Biang, 494 F. Supp. 2d 880, 890–92 (N.D. Ill. 2006) (same).

348 Whalen v. Roe, 429 U.S. 589, 591 (1977).

349 *Id.* at 599.

350 Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 138 (2011).

351 *See supra* Section II.C.

right to informational privacy.[352] It seems an entirely apt basis for applying the Constitution to require prerequisites to government collection of surveillance data.[353]

D. The Fifth Amendment

Finally, though some may deem it a stretch, the Fifth Amendment's Self-Incrimination Clause arguably applies to the collection of digital surveillance data as well. Benjamin Wittes writes about the phenomenon he calls "databuse," the "malicious, reckless, negligent, or unjustified handling, collection, or use of a person's data in a fashion adverse to that person's interests and in the absence of that person's knowing consent."[354] He calls out in particular the government's use of its authorities "to collect the components of a person's mosaic and then the use of those components against that person."[355] He concludes that this sort of databuse "is in some respects closer to the non-self-incrimination value of the Fifth Amendment than to the privacy value of the Fourth Amendment."[356]

There is something to the application of the Fifth Amendment to surveillance data collection. The elements of the Fifth Amendment are well established: A person must (1) be "compelled"; (2) to be a "witness" against oneself; (3) in a criminal proceeding.[357] Since the beginning, courts have held that the witnessing doesn't actually have to be in a criminal proceeding, just in a context that produces evidence that could be used in one.[358] Thus, to the extent the data could ever be used for law enforcement purposes, the third requirement is an easy one. The other two elements may seem superficially less evident, but let's give that some thought.

---

[352] *Whalen* has, in fact, been relied upon by lower courts for years. *See, e.g.*, Borucki v. Ryan, 827 F.2d 836, 839 (1st Cir. 1987) (relying on *Whalen* to assume right of privacy involves disclosure of personal matters); Patrick v. City of Chicago, 662 F. Supp. 2d 1039, 1061–62 (N.D. Ill. 2009) (relying on *Whalen* for the proposition that there is a confidentiality strand of privacy rights); Doe v. Magnusson, No. Civ.04-130-B-W, 2005 WL 758454, at *3–12 (D. Me. Mar. 21, 2005) (citing *Whalen* in tandem with other cases in discussing potential right to privacy); Conant v. McCaffrey, No. C 97-0139, 1998 WL 164946, at *4 (N.D. Cal. Mar. 16, 1998) (relying on *Whalen* to establish right to privacy). For more cases, see *supra* note 145.

[353] *See supra* Section II.C for a discussion of *Whalen*.

[354] WITTES, *supra* note 103, at 16.

[355] *Id.* at 2.

[356] *Id.* at 16–17.

[357] *See generally* Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857 (1995) (analyzing the main elements of the Self-Incrimination Clause: "person," "compelled," "in any criminal case," and "witness").

[358] WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, 1 CRIMINAL PROCEDURE § 2.10(b) (4th ed. 2021).

First, although one might argue that when the government collects our data, no one was "compelled" to do anything, *Carpenter* itself (albeit in the context of the Fourth Amendment) makes a perfectly persuasive argument to the contrary. Consider how the Chief Justice in *Carpenter* described using cell phones: They are a "pervasive and insistent part of daily life"; they keep records on us "without any affirmative act on the part of the user beyond powering up"; and "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[359] For that reason, he called into question whether turning over that data was "voluntary."[360]

As with the third-party doctrine, the Supreme Court uses a "voluntariness" test to cash out the Fifth Amendment's compulsion requirement, and what's true of the involuntariness of turning over CSLI is equally true of most government surveillance.[361] When it comes to DNA databases, or license plate reader databases, all we are doing is going about our ordinary chosen lives. It's untenable that we should have to abandon them to avoid disclosure. But as we lead them, inevitably dropping breadcrumbs about ourselves, the officials of the state stand behind us and off to the side, dustpans and brooms at the ready. Surely we are "compelled" to give up that data. As the Chief Justice explained in *Carpenter*, in the context of using cell phones, they are "such a pervasive and insistent part of daily life" that using one is "indispensable to participation in modern society," and "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[362] When it comes to DNA, or just traveling about, the options seem even more limited.

Finally, there's the requirement of being a "witness" against ourselves. The Supreme Court defines this element by drawing a distinction between "demonstrative" and "testimonial" evidence. Demonstrative evidence is things like providing a voice exemplar or putting on a glove, to show only that physical aspects of ourselves match up to what the government is trying to prove.[363] Testimonial evidence, on the other hand, is when we are asked to reveal something

---

359 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

360 *Id.*

361 For examples of the Supreme Court applying its voluntariness test, see Payne v. Arkansas, 356 U.S. 560 (1958); Watts v. Indiana, 338 U.S. 49 (1949). *See generally* Stephen J. Schulhofer, *Confessions and the Court*, 79 MICH. L. REV. 865, 867–78 (1981) (discussing the Supreme Court's "'old' due process voluntariness test" in the context of confessions).

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

363 *See* United States v. Dionisio, 410 U.S. 1, 5 (1973) (holding voice exemplars are nontestimonial); Holt v. United States, 218 U.S. 245, 252–53 (1910) (same; compelled donning of clothing).

about ourselves that would be unknowable but for the fact that we utter it.[364] Utterance, however, does not include only words; it is any sort of documentary evidence against ourselves that we create. *Marchetti* made that clear, stating that mandating that a person create and provide information to the government, such as when they go gambling, was a requirement "not significantly different from a demand that he provide oral testimony."[365]

It's certainly plausible that by collecting data we cannot help but to shed, the government "compels" us to be a "witness" against ourselves. First, there's a respectable argument, grounded in the scholarship of Richard Nagareda, and supported by Justice Clarence Thomas, that the testimonial/demonstrative evidence distinction itself is misguided, and that the Fifth Amendment covers any forced giving up of evidence to the government.[366] Second, one could argue surveillance data is testimonial. Some of our data, perhaps DNA that we shed, might fall on the demonstrative side of the line.[367] But much of it, most notably location data, could be understood as testimonial. It is how we create and describe the ways in which we live our lives. Consider, for example, if the government required us to keep a diary of our movements. That would surely be a violation of the Fifth Amendment. But how different is it really if the government monitors us to get the same information?

***

So there it is. Several different access points to the Constitution. It matters not a lot which one the courts seize upon, because the prerequisites of constitutional law that follow from choosing any of them are the same. That's the whole point of this Article, that some version

---

364 *See* Fisher v. United States, 425 U.S. 391, 411 (1976) (holding act of producing documents is testimonial if it provides government with new information regarding the location and existence of documents).

365 Marchetti v. United States, 390 U.S. 39, 57 (1968).

366 *See* Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575, 1623 (1999) ("The distinction is not . . . between testimonial communication and preexisting forms of incriminatory evidence. Rather, the fundamental distinction is between . . . the compulsion of a person 'to be a witness against himself' in the sense of *giving* self-incriminatory evidence—testimonial, documentary, or otherwise—and [the government *taking* such evidence]."); United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring) ("A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence.").

367 *See, e.g.*, United States v. Hook, 471 F.3d 766, 774 (7th Cir. 2006) (holding DNA nontestimonial evidence because it is a form of physical identification); United States v. Bean, 214 Fed. Appx. 568, 571 (6th Cir. 2007) (same); Kaemmerling v. Lappin, 553 F.3d 669, 686 (D.C. Cir. 2008) (same).

of those prerequisites applies almost any time the government demands personal information. There is no reason to think its content should vary by clause of the Constitution, as opposed to by the particulars of any data collection program. In my view special needs or *Whalen* provide the best hook. But unless mass government surveillance is to go entirely unregulated by the Constitution, which seems utterly implausible, any of these should do.

Conclusion

There are difficult questions around the proper use of surveillance by policing agencies. But the point of this Article is that courts need not confront them unless and until legislative (or other proper regulatory) action puts these government surveillance practices on a proper, lawful footing. If legislative bodies don't take that step—out of inertia, or because they are unwilling tacitly to approve the data collection that is happening—then courts should order that collection must cease, and the pools of data should be destroyed.

Some, I suspect, may say that requiring these prerequisites simply is not enough given the impact of surveillance technologies, but I think that is the wrong way to think about the problem. If legislative bodies do approve data collection programs, then courts still can assess their constitutional validity. That's exactly what the *Carpenter* Court did, striking down surveillance otherwise legal under the Stored Communications Act. But the courts have proven unable to deal with the problem of government surveillance. By forcing legislative bodies to act prior to government engaging in surveillance, courts perform the function of forcing societal dialogue over the question. When legislation is under consideration—openly and transparently, unlike much of the adoption of surveillance technology by policing agencies—advocates are free to argue for any outcome, from a ban to reasonable restrictions. The resulting legislation, if legislation is adopted, is the correct starting place for constitutional review. And if there is no resulting legislation, then surveillance should not occur at all.