A HOOVER INSTITUTION ESSAY

Private Data/Public Regulation

BARRY FRIEDMAN

Aegis Series Paper No. 2105

Introduction

Police collect information—that is what they do, and they could not do it without help. No doubt from the beginning of policing, officers have relied upon private parties to aid their investigations. Tipsters tip, snitches are paid, and well-meaning denizens share the information they possess. At crime scenes, police collect the names of people who may have seen something and follow up on those leads. And for the most part this has been, and remains, unregulated.

But there has been a sea change, brought upon us by technology, a change so dramatic it has transformed policing itself. Increasingly, the information police collect is digital. Fewer search warrants, more requests for orders to harvest metadata. Purchasing large pools of private data from data brokers. Capturing location information in various ways. Tapping into a network of private security cameras. And so on. Sometimes police collect the data themselves. More often they gather it from third parties. They do so from volunteers, by purchase, and by court order.[1]

The digital nature of the data allows it to be acquired in bulk. Rather than just focusing on the target of a particular investigation, the government can gather the information indiscriminately about large swaths of the population or even about all of us.[2] This was the case with the National Security Agency's collection of our telephone metadata, but it also is the case at the local level by automated license plate readers.[3]

The uses of this data are so broad that it is not just what we traditionally think of as the "police" who gather the data, but a variety of government entities involved in public safety and law enforcement. Bulk data collection has allowed law enforcement to shift its focus from a reactive investigative stance to a proactive and deterrent one. The police long have investigated particular cases, with suspects they had in mind or were trying to identify.[4] Now, government agencies utilize large databases to predict where crime will occur, or mine them for evidence of criminality.[5] This occurs without a particular suspect in mind and is aimed more broadly at the entire population or a segment of it.

No doubt this data collection has value, but precisely how much is an open question, and may depend in part on its use. For example, data collected from third parties, such as genetic information, has helped—to solve cold cases.[6] Facial recognition was vital to identifying the insurrectionists of January 6, 2021.[7] These are investigative uses. Here, the

value is plain, but the extent of that value unknown. The utility of bulk data collection for predictive or deterrent purposes is far more uncertain.[8] In truth there is far too little assessment of the utility of these new techniques, for whatever purpose they are deployed.

But one thing is clear: placing this much personal data in the hands of the government has its costs. It endangers our personal security, and our sense of privacy. It threatens our right to associate, including for political activity. It puts enormous power in the government to control behavior. And too often the collection is disproportionately of people of color.

I'm going to make a novel argument that, if adopted, would allow for capturing the benefits of data-driven policing, while mitigating its costs. My argument is that government agencies that engage in policing cannot collect digital data, particularly about individuals for whom there is no suspicion of wrongdoing, without a sufficient regulatory scheme in place. Thus, if these practices are to continue, legislative bodies must step in and adopt regulation.

What's novel about my argument is that I frame it in constitutional terms. I'm not just arguing that regulation is desirable as a normative matter. My precise claim is that *as a matter of constitutional law*, unauthorized and unregulated bulk digital collection of surveillance data simply may not occur. Absent such authorization and regulation, courts should invalidate such collection. More bluntly: with or without court intervention, government agencies involved in the policing function should cease immediately what they are doing until sufficient authorization and regulation is in place.

I support my argument by showing that in many contexts, under a number of constitutional amendments, when government seeks to collect personal information, courts impose a set of "requisites" before such collection is mandated or upheld. These requisites include that the collection of data is statutorily authorized, that it furthers a legitimate government purpose, that collection is minimized to protect privacy and personal security, that access to the data is safeguarded, and that judicial review is available to challenge the collection, retention, and use of such data.

Note that virtually all of this is missing from today's collection of surveillance data by government. That is what must change. I am not arguing government cannot collect the data, but that before it does, authorization and regulation by a democratically accountable body is essential. This puts the decision to collect the data, and minimal safeguards attendant thereto, in proper hands, rather than letting government policing officials simply decide for themselves.

Although I hope it has very basic normative appeal, my argument is a complex one with a number of moving pieces. I'm not going to have the space to lay it all out here, but I am doing so in other work.[9] In Part I, I will describe the phenomenon of widespread digital surveillance data collection that draws my attention. In Part II, I will sketch out my

argument, briefly but in full. Part III then will hone in on the body of constitutional law central to my argument, the cases I describe just above. Part IV will all-too-briefly touch on related parts of the argument and conclude.

I

I want to begin by briefly describing the developments that motivate the paper and to highlight two particular aspects. First, although many have expressed alarm that private companies are collecting and aggregating enormous amounts of data about us, governments are building similar databases on their own for law enforcement purposes. There may be benefits to all this, but there surely are costs. Yet, second, the Constitution as presently construed—particularly the Fourth Amendment—has proven of little value in regulating the practice of data collection, retention, and use. In the absence of constitutional regulation, there has been some legislative intervention, but far less than is necessary to cover the field or bring government surveillance data collection under the control it requires.

I.A

Policing agencies at the national and local level are building vast databases to keep tabs on us all. The FBI is constructing an enormous biometric database that will include facial images, iris scans, voice and palm prints.[10] New York is one of several cities with an extensive Domain Awareness system, which collects and aggregates information from a network that includes over 9,000 cameras, 500 license plate readers, and data from government databases.[11] 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: by surreptitiously nabbing beverage cups from people they suspect, to asking consent from victims or people they wish to clear in investigations, and then retaining it.[12] The police use technology like from the company Cellebrite to vacuum up the contents of cell phones during routine searches, and hoard it for later use.[13]

Not content with their own data collection efforts, however, policing agencies increasingly are relying on private data sources to monitor or provide information about the public for them. One of the largest is the CLEAR database maintained by Thomson Reuters, which advertises CLEAR as a "[p]owerful public records technology" that "brings all key content together to provide intelligent analytics in one environment."[14] That database compiles extensive information on people's credit, employment, and so forth. A recent story told how ICE was using CLEAR to trace undocumented individuals using utility usage information.[15] Thomson Reuters is not alone; another recent news story related how ICE apparently is switching data vendors, moving over to the database run by LexisNexis.[16]

Databases that track our location are particularly illustrative of the public-private partnerships in this space. Automated license plate readers (ALPRs) provide an excellent example. ALPRs sit on police cars or other vehicles, or are mounted in fixed locations, and

they suck in the license plates of motorists around them, geolocating where those cars are at that moment.[17] Originally the point of ALPRs was to compare the reads to a "hot list," such as to detect stolen vehicles.[18] But law enforcement agencies soon decided there was value in retaining the reads in case they proved useful later in a criminal investigation.[19]

Many departments now use ALPRs extensively, both to create huge databases of where automobiles have been when, and to geofence their communities so they know who is coming and going. Axon, the leading U.S. seller of body cameras and Tasers, is releasing a new digital ALPR system that turns ordinary police car dash cams into powerful tools that can collect reads from traffic across three lanes, front and back, as police cars move on patrol.[20] The LAPD has a database of some 320 million license plates that it stores for at least five years.[21] Myrtle Beach, South Carolina, keeps tabs on visitors with ALPR cameras covering all exit and entrance points to the shore town. In 2019 those cameras captured almost 40 million reads.[22]

But policing agencies have expanded their capabilities substantially by linking up with private vendors to create a network of tracking and tracing capability. The industry leader in this space is Vigilant, owned now by Motorola Solutions, which advertises and makes available to policing agencies a database of over 500 billion stored geo-located records. Vigilant's database is fed with license plate readers attached to repo trucks, but also garnered from policing agencies that turn their information over, often in return for access to the larger pool of data.[23]

I.B

These public-private partnerships may have real advantages for policing agencies and for public safety, but one pervasive problem in this area is the lack of any systemic attempt to identify those benefits. Cops will offer up anecdotes about the time ALPR evidence helped crack a case, but we don't know if the ALPR was essential, or how valuable it proved, let alone how often that was the case. There are well-known examples about how reliance on third-party data helped crack notorious cold cases, such as that of the Golden State Killer.[24] But how often does this happen? If we are going to allow the government to create or rely on third parties to provide huge aggregated databases, it seems incumbent upon government to prove the value. I will return to this point below.

For now, though, I want to focus on the harms from this sort of data aggregation, because they are what make the case for regulation. If benefits were uncertain but harms nonexistent, our only concern would be the potential squandering of government resources. The loud pushback we hear today against government collection and use of private data suggests much more is at stake.

First, there are the threats from errors in these databases, and though error is a small word, the danger here is enormous. These mistakes cause people to become law enforcement

involved, and the news at present is all too clear about the risks those police encounters pose. At best they are an intrusion on liberty and psychologically stressful; at worst they end up in police shootings or other uses of force. Albert Florence was picked up for an outstanding warrant on a fine that had been paid but erroneously recorded as open. "He spent seven days in jail" and "was strip-searched twice" in that time.[25] Robert Julian-Borchak Williams suffered a similar false arrest, this time because a facial recognition algorithm (with a human supposedly in the loop) wrongly ID'ed him for shoplifting from a high-end boutique. Despite his denying the image was him he spent 30 hours in jail, and his wife had to claim an "emergency" to his employer lest he risk losing his job.[26] It is impossible to know the magnitude of these "errors," but one can reasonably estimate that there are tens if not hundreds of thousands of stale or erroneous warrants sitting in databases waiting to result in a wrongful arrest.[27]

Second, there's misuse of the databases, just the kind of thing you'd expect when you leave huge stores of personal information lying about. 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."[28] All too often there are stories of policing personnel dipping into the databases to spy on people with whom they have personal issues—frequently stalking intimate partners.[29]

Third, and perhaps most important, allowing government to accumulate and have easy access to detailed dossiers on all of us threatens our personal and collective security.[30] There are always those eager to argue it can't happen here, but it can—and too often it has. 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 all too often attempted to intervene in ways that were insidious to democracy.[31] "Fusion centers"—federally supported state and regional intelligence-gathering hubs, often relying on privately collected data—repeatedly have been caught spying on entirely lawful First Amendment activity.[32] Even if we accepted the purity of government watchers—as I do, for example, of the National Security Agency's vast data grab revealed by Edward Snowden—it's inconceivable that we want government to have access to all this data without public debate and adequate regulation.

Although this sort of surveillance can fall upon all of us, it's undeniably the case that when the government determines to collect and use information against people, there's a good chance those who suffer most will be Black and brown.[33] It's not a surprise that Robert Williams and Albert Florence were Black.[34]

I.C

The simple fact is that most government surveillance data collection, by policing agencies or via third parties, is profoundly under- or unregulated. The Constitution as presently interpreted offers almost no protection to the sort of widespread data collection by the

government.[35] There is some legislation in this space, such as the federal Electronic Communications Privacy Act and various state and local laws, but most of it is already outdated, and in general what police and private data collectors do happens without any regulation. As Benjamin Wittes writes, aptly, "[m]ost of this data is not plausibly protected by the Fourth Amendment. Much of it is not protected by any law at all."[36]

Absent a small niche doctrine of "private searches" the Constitution doesn't apply at all when the government acquires personal information from private parties. The Constitution for the most part binds public actors, not private ones. The private search doctrine holds that unless a private entity effectively was "deputized by state officials ex ante," to search or seize, the government will not be held accountable for the action.[37] As one of the leading cases in the space put it, the Fourth Amendment applies only to "governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'"[38]

The larger difficulty is that even if the government is collecting bulk surveillance data, the Fourth Amendment—the only constitutional provision that does any work in this space—still has very little to say about it.[39] Ironically, the Supreme Court in cases involving "innovations in surveillance tools" has taken to insisting that no matter what else the Amendment may or may not do, it "assure[s] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[40] That is not remotely true.

The threshold triggers for the Fourth Amendment are that police conduct must be a "search" or "seizure," and most surveillance data collection never gets past this point.[41] First, most of what you do in public, which is to say could conceivably be viewed by someone in public, is not deemed a search.[42] So, for example, in twinned cases—*United States v. Knotts* and *United States v. Karo*—the Court held that using a beeper to track someone to the end point of a journey on the highways was not a "search."[43] Second, under the "third-party doctrine" anything the government collects that you have given over to a third party also is not a search.[44] That includes bank records, phone numbers dialed, papers given to an accountant, etc.

In two relatively recent cases the Supreme Court has held that long-term location tracking can constitute a search, but like all exceptions these cases prove the rule of constitutional neglect. In *United States v. Jones* the justices relied on the physical trespass of installing a Global Positioning System (GPS) on a car to collect information as the basis for concluding it was a search and that a warrant was required.[45] More important for present purposes, five justices in *Jones*—concurring—held the better analysis was that long-term location tracking was a search, even if the sort of short-term tracking at issue in the *Knotts* and *Karo* cases was not.[46] Then, in *Carpenter v. United States*, the justices concluded that using a court order to acquire seven days or more of cell site location information also was a search.[47]

Those decisions were a step in the right direction, but it was a baby step at best and leaves most of what we are concerned about uncovered by the Fourth Amendment, even if the police themselves collect it. First, note the weird lines being drawn: 30 days of GPS tracking is too many; same for seven days of CSLI. The justices are grasping at straws to get invasive digital data collection under control, but they really are struggling. Second, as Justice Kennedy, dissenting in *Carpenter* rightfully points out, why location tracking and CSLI, but not all the other data given over to third parties, like our credit card purchase, or bank records, or bills from therapists and medical clinics?[48] There's no decent answer to this question and the majority offered none.

The justices are not oblivious to the problem; they just don't have a solution. The *Carpenter* decision was full of alarm about what these sort of data grabs could accomplish. The Chief Justice—writing for the majority—described "the seismic shifts in digital technology"[49] that today allow the government to "achieve[] near perfect surveillance."[50] Not just in the here and now, he pointed out, but retrospectively. "[T]he Government can now travel back in time to trace a person's whereabouts," giving "police access to a category of information previously unknowable."[51] And not just for criminal suspects—"this newfound tracking capacity runs against everyone."[52]

Many commentators, and even the justices themselves, have called upon legislative bodies to step in and regulate surveillance technologies, but for the most part the sort of data collection discussed here is entirely unregulated. Some states have laws governing license plate readers; most do not. There are state laws governing DNA databases, but policing agencies have circumvented them by creating unregulated local ones.[53] The data broker business is for the most part unregulated. So too the use of mobile forensic data terminals like Cellebrite. The list of what receives no regulation far exceeds what regulation there is.

II

In general, the right answer to the vacuum surrounding government surveillance data collection is legislation, not constitutional law. Data collection of the sort we are discussing has many facets, all of which require regulation. Here is a short list of things that need to be addressed, and it is hard to see constitutional law doing the trick: What data can be collected? On whom? How long can it be retained? What is the predicate for accessing the data? What is the security for the data storage? What sort of auditing should there be. And so on. These are not the sort of fine-grain questions constitutional law addresses. Legislation can and should.

The problem is that legislators have little incentive to pass the sort of legislation that is needed. Doing so will anger powerful police or prosecution lobbies or leave them vulnerable to later claims that they were soft on crime. There is a vast literature on this.[54] And it is why most of the collection of surveillance data remains unregulated.

What constitutional law could do is motivate legislative action. Two things tend to overcome legislative inertia to do nothing: highly salient cases that motivate the public to call for regulation, and court decisions that force legislation. An example of the former is how the reaction to Edward Snowden's revelations caused Congress to adopt the USA-Freedom Act, taking the data out of NSA hands and requiring a court order to access it.[55] An excellent example of the latter is how the Supreme Court's decisions in *Berger v. New York*[56] and *Katz v. United States*[57] motivated the federal wiretapping law.[58]

What I want to argue is that constitutional law not only could motivate such legislative regulation of surveillance data collection, but that it must. It would, in effect, operate as a "penalty default" rule, changing the status quo from "collect, and legislatures can regulate if they wish" to "before any government agency can collect this data, there must be legislative regulation."[59] There are four parts to my argument, all of which are complex in their own right. I've not got the space to discuss them all fully in this piece. I intend to hone in on the first part of the argument, and summarize the rest. But before I do, I want to lay out the full argument briefly, so that its arc is clear.

First, in many other areas in which government collects information about private individuals, the Constitution lays out a set of "requisites" before that data collection can proceed. Cases arise under various clauses of the Constitution (including the Fourth Amendment). They arise in the criminal and in the civil context. They involve collection by the federal government, but also by state and local governments. Across all these areas there is a remarkable commonality of what courts—and especially the Supreme Court—say must be in place for the collection, retention, and use of the data by the government. Courts require that data collection be authorized, that it be for a legitimate purpose, that the collection further that purpose, that when privacy is at stake the need for the regulation outweigh the costs of intruding on privacy, that there be procedures in place to minimize unnecessary collection, and to safeguard against inappropriate disclosure.

Second, the only reason that government surveillance data collection escapes the embrace of ordinary constitutional law is because—as we saw above—the collection itself is not considered to implicate the Constitution at all. The second part of my argument is directed at this claim.

The short answer is that constitutional law evolves constantly in the face of technological change, especially in the area of government surveillance. As I've indicated above, wiretapping was entirely outside the Constitution, until the Supreme Court pivoted. So too with location tracking on open roads. There are many other examples and Fourth Amendment law is full of them. What I show in other work is that there are no fewer than six different ways to bring bulk digital surveillance data within the Constitution, none of them revolutionary.[60] And that the cost of doing so is not to impede collection by the government, but only to require it occur pursuant to legislative regulation.

The argument thus far speaks to government collecting data on individuals, not to private companies doing so, which raises the question of what should happen in the latter instance. Many today are calling for regulation of private data collection, for example by data brokers. It seems appropriate to consider such regulation, but that is neither my mission here nor do I think it will be adequate to the problem. Yes, Thomson Reuters, LEXIS, and all the rest should be regulated. But many entities that are not considered primarily in the data business nonetheless are a rich source of data for law enforcement.

The better answer is to regulate law enforcement itself, and its access to such data. That is the third step in my argument. Which is to say, in general terms the constitutional argument I am advancing here should apply to government acquisition of surveillance data, no matter whether government acquires the data itself, or gets it from third parties. The details may differ—undoubtedly they have to. But as the survey of cases in which we will soon embark makes clear, the constitutional requisites apply whether the government collects data by way of subpoena, other court order, administrative program, or legislative program.

Finally, there is the question of what precisely constitutional law should require of legislative bodies. What are the requisites of constitutional law regarding government collection of surveillance data? Once again, full explication of the answers will have to await other work, but superficially the answers are not complicated, and will emerge from the cases I discuss next. They are the very requisites identified above, from legislative authorization to gather hold and use the data, to how it is secured. The case law makes all of this reasonably clear.

So that's the argument: before government can collect surveillance data in bulk, the Constitution requires an adequate regulatory scheme. This follows logically from the cases I'm about to discuss at some length. It works no revolution in constitutional law to apply that case law to government collection in bulk of surveillance data. But it does accomplish one essential thing: limiting the ability of executive officials, and in particular police departments, from deciding on their own how they are going to surveil individuals, especially those for whom they have zero evidence of lawbreaking. Back in the day when policing was investigative and aimed at suspects, and the technological tools were limited, such legislative go-ahead may not have been necessary. In an age of sweeping, indeed breathtaking surveillance, it's time to require our democratically accountable representatives to step up and do the decision making.

III

In this first part of my argument, the one I will develop most here, I am going to take you on a whirlwind tour of the Constitution, in which we will see that in many circumstances in which the government collects private information for law enforcement purposes, courts require a variety of requisites.

III.A

We'll start, ironically, with another corner of the Fourth Amendment, the use of subpoenas in government investigations. There are two advantages to this starting point. First, subpoena practice is a ubiquitous method of gathering individual information for public use, and quite in contrast to the sort of data collection we are concerned with, it is regulated. Second, it is useful to see that the sorts of requisites we care about are not alien to the Fourth Amendment, but are in fact familiar ones.

Initially it seemed like using subpoenas to access private information for use in criminal proceedings might be ruled out altogether, but the Supreme Court quickly did an about-face when it became clear such a rule would shut down the administrative state at its inception. In *Boyd v. United States* in 1886, the Supreme Court held, famously, that the Fourth and Fifth Amendments together prohibited a subpoena of a person's private papers in a criminal forfeiture proceeding.[61] "[P]apers are the owner's . . . dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection. . . ."[62] The response, which ultimately made headway, was that there was no search, because 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 offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property. . . ."[63]

Although *Boyd* was brushed aside in the 1906 case of *Hale v. Henkel*,[64] the Court nonetheless made clear the Fourth Amendment governed the use of compulsory process to gather private information. "[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," said the Court.[65] For that reason, no warrant or probable cause would be required. Still—and this was the important point—the use of the subpoena was a search within the meaning of the Fourth Amendment. For that reason, certain legal requirements had to be met so that use of the subpoena was not "unreasonable."[66]

The 1946 decision in *Oklahoma Press v. Walling* was the watershed, setting out the three chief constitutional requirements imposed by the Fourth Amendment for an "order for production" to be valid.[67] First, there was the question of statutory authorization; a subpoena only is permitted if it is for "an investigation[] authorized by Congress."[68] Second, it had to be "for a purpose Congress can order."[69] Finally, the documents requested had to be "relevant to the inquiry."[70] *Oklahoma Press* was a federal case, but given that the Fourth Amendment applies equally to the states, some legislative body must authorize subpoena practice there.[71]

In practice, courts apply the *Oklahoma Press* requisites generously in the government's favor, but the bounds still are real ones, particularly the requirement that the information

collected be relevant to a lawful purpose. In *FTC v. American Tobacco Company*, Justice Holmes laid down the law that governs to this day.[72] "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."[73] The *Oklahoma Press* Court reiterated the point (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. . . ."[74]

Relying on these principles, courts have invalidated subpoenas that stepped beyond the bounds of what a statute authorized, or that requested documents that did not seem related to the authorized investigation. The Fourth Circuit struck down the IRS's practice of using a tester to see if an accountant was filling tax returns properly, and if not then issuing a summons for every return filed by that accountant.[75] "The [IRS] is not to be given unrestricted license to rummage through the office files of an accountant in the hope of perchance discovering information that would result in increased tax liabilities for some as yet unidentified client."[76] These summons "are not meant to serve as a tool to police the accounting profession."[77] And when the Resolution Trust Corporation attempted to subpoena information on the net worth of officers and directors of failed Savings and Loans, courts balked. Typical was a decision concluding that "not all of the information sought by the RTC is relevant to the issue of liability. Much as we strain our imagination, we cannot find a 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."[78]

Courts are even more strict when private (as opposed to business) information is collected, and stricter still when it is from people to whom no suspicion attaches. Indicative are cases in which the government agencies tried to locate assets pilfered from failed financial institutions by subpoenaing private financial information from former officers. "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."[79] The Second Circuit, in a case involving the FDIC, held that although in general the government's appraisal of relevancy "must be accepted so long as it is not obviously wrong"[80] still, "[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. Conjugal or familial association with a corporate participate does not, by itself, strip an individual of his or her expectation of privacy."[81] For this reason, 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."[82]

The basics are thus clear: government has broad power to investigate, but the power must be exercised in ways that meet some essential requisites. To be "reasonable" and thus

constitutional under the Fourth Amendment, no warrant is necessary but: (a) formal statutory authorization is required; (b) the request must be in service of a legitimate governmental goal; (c) the information sought must be relevant to that legitimate goal; (d) the relevance requirement fails when there is no ongoing investigation into wrongdoing for which the information is requested; (e) the burden of showing relevance is higher on the government when the private information of individuals—rather than corporate information—is at stake, especially if those individuals are accused of no misconduct; and (f) courts are available to ensure these rules are followed.

There's one last point, so obvious as to escape notice, and yet critical. All of this happens pursuant to judicial supervision. Not only must the government meet certain requirements, but before information is compelled, there must be a hearing at which the recipient "may challenge the summons on any appropriate ground."[83]

Again, these are requirements under the Fourth Amendment, and as we've seen much bulk collection avoids that as it is deemed not a "search." We'll get to that in Part III, but for now focus on what courts do require when the Constitution applies. That's the point of this Part.

III.B

Slide over to the Fifth Amendment and things look remarkably similar. Our example here will be the "required records" doctrine. The government frequently requires us to keep records, and at times it also requires reporting. But the precise same sort of requirements and limits we just saw also apply if keeping that information and turning it over to the government might lead people to incriminate themselves.

The required records doctrine found its root in *Shapiro v. United States*, a case in which a fruit and vegetable purveyor challenged use of information he provided pursuant to subpoena, when he was indicted under the Emergency Price Control Act.[84] The Act required him to keep records of business transactions. He argued that having complied with the subpoena, using the information—rather than immunizing him from prosecution—would violate his Fifth Amendment right to be free of compelled self-incrimination. He lost on the theory that the documents in question 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."[85] Were this not the case—were the documents "private papers"—then the privilege would have applied. Justice Frankfurter, one of the dissenters, was apoplectic at the conclusion that these sorts of papers were "public" in any sense. "If records merely because required to be kept by law *ipso facto* become public records, we are indeed living in glass houses."[86]

The required records doctrine soon met its constitutional match in a case called *Marchetti v. United States*, which limited *Shapiro* to keep it within constitutional bounds.[87] Marchetti

was a gambler who balked at certain statutorily required reporting of his activities, on the ground it invariably ended up in the hands of local prosecutors. The Court agreed, distinguishing *Shapiro* on a number of grounds, primarily that the gambling records the statute required Marchetti to keep were not "of the same kind as he has customarily kept," but that he was required to create and provide information to the government to be used in a criminal proceeding—a "requirement . . . not significantly different from a demand that he provide oral testimony."[88]

Shapiro and *Marchetti* together make evident four requisites for government collection of personal data, three of which are going to sound very familiar. First, there had to be statutory authorization to collect the information. In *Shapiro* the Court began: "[t]he record involved in the case at bar was a sales record required to be maintained under an appropriate regulation. . . ."[89] It stated that its rule would not apply to information "whose keeping as records has *not* been required by valid statute or regulation."[90] Indeed, this is what gave the information its status as a "public record."[91] And second, the information sought had to be relevant to the valid statutory scheme. Again, in *Shapiro*, "there 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 particular records. . . ."[92] On the other hand, the government could not require turning over data if it is "plainly incompetent or irrelevant to any lawful purpose."[93]

Marchetti then added the rule that held government could not collect the information if its aim was criminal liability, rather than a regulatory purpose. *Marchetti* distinguished *Shapiro* because there the information requirements were imposed in "an essentially non-criminal and regulatory area of inquiry."[94] Similarly, in *Grosso v. United States*, a companion case to *Marchetti*, the Court began its description of the three factors that distinguished valid required records saying "the purposes of the United States' inquiry must be essentially regulatory. . . ."[95] The gambling tax rules were invalid because "the statutory obligations are directed almost exclusively to individuals inherently suspect of criminal activities."[96]

Finally, unstated but evident—as in the area of Fourth Amendment subpoena protections—the government effort to get the information had to run through lawful judicial process. The government could not simply come take the information, or even demand it and just expect its production. Whether challenged before providing the information, or at the time the information was used in a criminal proceeding, collection of the information was subject to judicial review.

Thus, the rules under the Fifth Amendment look very much like those under the Fourth when the government is subpoenaing private information.

III.C

We can move away from criminal investigations of individuals now, to more generalized requests for information, starting with what typically is referred to as the "right to privacy." There were many motivations for the emergence of the right in the 1970s, but one of them was computerization of data. In *United States v. Westinghouse Elec. 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."[97] In 1974, Congress enacted the Privacy Act, which regulated the collection, management, and use of private data.[98] But it did not apply to the states, and had an exception for law enforcement, and so the right became constitutionalized to fill in some of the gaps.

Whalen v. Roe is the seminal case dealing with the "right to privacy." *Whalen* involved a New York statute requiring physicians to report and New York to store information regarding the prescribing and dispensing of controlled drugs.[99] That very same year the Court decided another privacy case, *Nixon v. Administrator of General Services*, in which the former president challenged on constitutional grounds a congressional statute providing a process for the curation of his private papers in order to determine which should be returned to him and which should become part of the public record.[100]

As usual, the first order of business when government is collecting personal information that implicates the right to privacy is statutory authorization. New York's law, the *Whalen* Court explained, was "manifestly the product of an orderly and rational legislative decision."[101] 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. . . ."[102] Similarly, the *Nixon* Court repeatedly stressed that the review of the former president's papers was pursuant to congressional statute and that the Act was "a reasonable response" to a "difficult problem" of intermingled private and public papers.[103]

Given that these cases involved not an investigation of an individual for possible criminal or civil liability, but a broader information gathering exercise, the requirement of relevance is discussed in the cases as a matter of legislative justification. Recognizing that "[s]tates have broad latitude in experimenting with possible solutions to problems of vital local concern," the *Whalen* Court nonetheless engaged in an analysis of the various state interests that supported the law.[104] The law at issue was a "considered attempt"[105] to "minimize the misuse of dangerous drugs."[106] "It was recommended by a specially appointed commission which held extensive hearings on the proposed legislation"[107] and "the State's vital interest in controlling the distribution of dangerous drugs would support a decision to experiment with new methods of control."[108]

Much like the heightened scrutiny applied to subpoenas of private information, courts dealing with right to privacy cases often go further and require efforts to minimize or

avoid intrusion on personal privacy.[109] *Westinghouse* was a subpoena case, but with a twist: 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. Although a balance of interests justified releasing the information to the government, given that "there may be information in a particular file which an employee may consider highly sensitive,"[110] 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."[111] The *Whalen* Court explained it was not "unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[112] The Court detailed the security around the computerized information, and made clear it was not deciding any question involving "a system that did not contain comparable security provisions."[113]

III.D

I could go on. There are similar cases arising under the First Amendment and even the Second Amendment, and in truth a wide variety of types of cases.[114] In my longer work I collect these at great length. What we see is that time and again when the government seeks to obtain private information from individuals, courts expect the government to meet some basic requisites. The collection must be authorized by statute. It must be justified by a legitimate (at least) government purpose. The collection must advance that purpose, and not be a fishing expedition into people's lives. The more private the information, the greater the burden on the government including to minimize collection when unnecessary. There must be safeguards to protect against disclosure of the information. Judicial review must be available.

IV

These sorts of requisites are familiar throughout constitutional law, but they are almost entirely absent from the government's collection in bulk of digital surveillance data. At present, the government can and does obtain our personal information, including information that can be quite revealing of our lives, based entirely on the decisions of executive and policing officials. We have little choice but to live our lives, and as we do the government surreptitiously goes about collecting the digital breadcrumbs that we drop.[115] There is no regulation and little oversight. This is true whether the government collects and retains our data or acquires it from third parties.

My hope is to have persuaded readers that allowing this sort of collection to continue unregulated both is normatively problematic and a deviation from the texture of the law. I want to emphasize that I am not saying government should be barred from collecting the information. That would have to be resolved on a case-by-case basis, depending on if the government can meet the requisites set out above with regard to any particular collection. But what I am sure of, and hope others agree, is that it simply is unacceptable to allow such collection, retention, and use to continue absent a regulatory scheme that meets the basic

requisites. (And I strongly suspect—and hope—that if legislation is required, the hoovering of personal data that is currently going on will be curtailed sharply.)

In this final part, I want to deal briefly with three pieces of a longer argument. They are: the constitutional basis for requiring (as opposed to preferring) regulation of the collection in bulk of surveillance data, whether the rules should differ if the government is acquiring the information from third parties rather than collecting it itself, and what exactly regulation looks like.

IV.A

It's one thing to believe that regulating the collection of surveillance technology is a good idea, and quite another to take the position that the failure to do so is unconstitutional. I'm of the latter view. It matters: if collection implicates the Constitution then what is occurring at present is unconstitutional, and must cease until there is regulation.

The stumbling block to the constitutional argument is the Supreme Court's Fourth Amendment doctrine, which holds that most of surveillance data collection is not a search. At present the analysis begins and ends there. But that answer is just too simplistic and uncreative.

Elsewhere I offer six different ways the Constitution could be called into action—and should be—to ensure the basic requisites identified here apply to government's bulk collection of digital surveillance data.[116] They vary in their plausibility under existing doctrine, but none is out of bounds, and some are quite sensible and straightforward, such as *Whalen*'s right to privacy. I'm only going to hone in on a couple here, both arising under the Fourth Amendment—the question of what is a "search" and the Supreme Court's "special needs" doctrine.

Before I spell the doctrinal arguments out, though, I want to offer up what I believe are the real obstacles that have held courts back. I don't think those obstacles are doctrinal, so much as they are more practical and consequential. As I said earlier, constitutional law regularly changes in the face of technological evolution, and especially around police surveillance. *Katz v. United States* overruled prior decisions and made warrantless wiretapping unconstitutional. *Jones* and *Carpenter* limited *Knotts* and *Karo* in terms of tracking people on public roadways. *Kyllo v. United States* said the police can't use emerging technologies to learn what is going on in our homes.[117] *Carpenter* itself seems to adopt the view that what is a search depends on the intensity of the surveillance, and the quantity of information gained, which opens up a whole new examination of government information gathering.

The real obstacles to bringing surveillance data collection within the Fourth Amendment involve questions of line-drawing and of consequences. As to the first, it is clear from *Jones* and *Carpenter* that the justices are having trouble saying how much is too much. This is the

inevitable difficulty with making the decisions turn on intensity and quantity. And that difficulty is compounded by the fact that—as the justices well understand—if a warrant is required for the collection of all surveillance data, then many investigations will not get off the ground at all. So the justices understandably are concerned about tying the hands of law enforcement. The latter difficulty is particularly acute, because if the Supreme Court bars a practice under the Constitution absent a warrant, that decision will stick unless and until the Court overturns itself.

But note how my argument solves the justices' problems, to such a degree that they may warmly adopt it. It allows the justices to duck the "how much is too much" problem by remanding surveillance issues to legislative bodies and letting them have a first crack at the question of what data collection should be permitted. This makes huge sense. Legislative judgments will make more tangible the question of law enforcement necessity. Legislative programmatic decisions will provide the justices with a broader perspective than taking up seriatim individual instances of law enforcement collection.

More important, adopting my argument would not permanently take any surveillance technique out of law enforcement hands (absent probable cause and a warrant). It simply requires the sort a legislative judgment about whether the collection is permissible. And at least as an initial matter (subject, of course, to judicial review), a legislative body can determine whether a warrant and probable cause is required, or not.

To the extent the formulation here is congenial with the justices, getting there doctrinally is much easier than it may look at present. It hardly betrays the English language to call the bulk collection of surveillance data a "search." If, for example, the government is tabulating the location of my vehicle, or nabbing my DNA surreptitiously, it is not much of a stretch—if a stretch at all—to bring that within the Fourth Amendment. The superficial problem may seem to be that if such collection is a search for the purpose of requiring regulation, why not also for the purpose of requiring warrants? In other words, once this sort of collection is deemed a search, doesn't the warrant requirement necessarily come along with it? But that question already is answered in the negative in the doctrine. As we saw in Part III, subpoenas are "searches" for Fourth Amendment purposes, but they only need be "reasonable," and no warrant is required. Why not the same approach for programmatic collection of surveillance data? The Court easily could distinguish collection in targeted investigations from collection in bulk.

Indeed, there is an entire body of Supreme Court doctrine devoted to programmatic government searches, which also could be called into play here: the "special needs" doctrine.[118] The Supreme Court has held repeatedly that if a search or seizure is not for ordinary law enforcement, but a special need of public safety, then warrants and probable cause are not necessary (at least in the traditional sense) and an entirely different set of rules apply.[119] Examples are sobriety checkpoints and airport security, neither of which requires a warrant

or probable cause.[120] This "special needs" approach seems the logical way to address bulk surveillance data collection. Under the special needs doctrine, the Supreme Court employs a balancing test weighing the government need against the individual interest to determine if the government's program is constitutional.[121] But some of those cases also talk about "adequate safeguards" to replace a warrant,[122] and that seems the logical place to house the requirements of legislative authorization and regulation. In fact, many of the special needs cases already refer to such legislative authorization and regulation.[123] It would not be much of a move to bring bulk surveillance data collection within the special needs rubric.

The fundamental point is that there are available constitutional hooks for the regulatory approach I advance here. Yes, some doctrinal evolution is required. But that is not unusual in the surveillance space, and the justices may well welcome taking this step as it eases the burden they currently are facing in figuring out the bounds of *Jones* and *Carpenter*.

IV.B

So far, much of the argument has been about government collecting surveillance data on its own, rather than turning to third parties to acquire it. Yet, as we have seen, one of the primary vehicles for the government collecting and using surveillance data in bulk is acquiring it from such third parties. This can be by purchase, such as from data brokers, or by court order, such as is current practice with regard to mobile phone cell site information. The question is how this acquisition from private parties should be regulated.

There's a pretty simple answer to this question—you may already have surmised it—but before spilling the beans, it's worth noting that it is an open question whether it is better or less good that law enforcement would collect information itself as opposed to acquiring it from private third-party entities.

On the one hand, private vendors are likely to have much more information than any given agency could compile (with the exception, perhaps, of the Federal Bureau of Investigation). This may be seen as a good thing, and may be seen as a bad one, depending on where one sits, but it is a fact. If the point is to use data to foster public safety, more information might be better. If one is worried about overweening surveillance, it might be a problem.

On the other hand, it actually may be more protective of individual rights and liberty—i.e., may avoid some of the harms discussed in Part I—if the data sits in private hands. If overweening surveillance is the fear, not having the data sitting in governmental hands is a good thing, not a bad one. That actually was the decision Congress reached when it adopted the USA-Freedom Act in response to Edward Snowden's disclosures.[124] The telephone metadata at issue was taken out of the NSA's hands, and left to rest instead with the providers.[125] The NSA only could access it with a judicial order based on the requisite level of suspicion. *If* we are going to allow the government to access stores of information,

particularly for use in criminal investigations, this might make a lot more sense than allowing the government to collect and aggregate the information itself, and dip into it as it wishes, with no safeguards.

In any event, the general answer to our question should now be clear: legislative regulation. If the government can't collect the data for its own use without a legislative scheme in place, it hardly makes sense to allow it to acquire that data otherwise in a way that circumvents the regulatory requirement. Many people are advocating regulation of the private data collectors, but as I see it, the proper party to regulate is the government itself. That is not to say private data collection should remain unregulated, but imposing such regulations poses special challenges. If the concern is government conduct, the direct solution is to regulate the government itself. Regulation of acquisition of data by government from private entities may prove to be a more complex matter than regulating government collection, requiring more elaborate rules. Danielle Citron and I are working through what that should look like. But our instinct is that the sensible approach is to regulate government acquisition. That can create harmony among methods of acquisition, be they by the government itself or from private entities.

IV.C

If I'm right so far, then policing agencies cannot—and no longer should be permitted to—collect surveillance data in bulk without legislative authority, then the question becomes, what should this look like? Again, I lay this out in detail elsewhere, but here's a peek.

At present the most difficult questions rest around statutory authorization. Many of the cases treat as the first requisite that collection be pursuant to such authority. But what does it mean to be authorized? Most policing agencies are chartered, and so courts would have to struggle with whether a grant (often made long ago) to do such things as "keep the peace," "enforce the law," or "maintain order" suffice to adopt technologies like facial recognition and DNA collection.[126]

But the difficulty of this question evaporates if legislative regulation is required. If that is the case, it likely will be much clearer not only the rules by which collection occurs, but what the legislature has authorized to be collected. This, ultimately, is just one more point in favor of such legislative schemes.

As to what a statute *must* contain, the law on requisites really does lay out a road map. Government must make clear why it is collecting the data. It must not collect it if the data does not further a legitimate (or compelling, depending on what right is implicated) reason. Government may not collect more data than is needed for its purposes, and must minimize its collection and retention. The data must be safeguarded in terms of who can access it, and

how easily. There must be judicial review of the surveillance data program. At a minimum, statutes authorizing the collection of surveillance data in bulk should address these issues. They should spell out clearly the collection that is permitted and its purposes, and have provisions to minimize unnecessary collection, to safeguard and limit access to the data, and to provide for legal challenges to collection.

Of course, that's not a full regulatory scheme for data collection; there are many other features that a legislative approach should address. These include things like how long data can be retained, what predicate if any is required to access it, what individuals should have access and what training is required of them, what auditing mechanisms must exist, what must be disclosed to the public, and the like. These may or may not be required as a constitutional matter. But my hope is that as the idea of regulating surveillance data by statute becomes normalized, a set of best practices for such regulation will develop.

Indeed, the more I think about all this, the more I've come to believe what each state needs is an omnibus statute regulating surveillance data programs generally. It can't make sense to have one statute for DNA data, another for ALPR data, another for MDFT data and the like. There may be the need for specificity about particular technologies, but we as a society should think deliberately and comprehensively about what data we want the government to acquire, hold, and use, and according to what rules. And those rules should apply across data sources, at least in general terms.

• • •

In any event, what does seem to me imperative is to have this conversation and make deliberate decisions, not simply glide into a surveillance state. Constitutional law could do a lot of work in that regard, forcing legislative deliberation. That's the point of this piece. The law is not here yet, of course. But I hope to have persuaded that it should be, and could be, without a lot of effort or disruption.

NOTES

1 *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 (discussing law enforcement agencies' practice 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-your-digital-data (cataloguing the types of consumer data that the government can obtain through subpoena); Sidney Fussell, *How Your Digital Trails Wind Up in the Police's Hands*, WIRED (Dec. 18, 2020, 7:00 AM), https://www.wired.com/story/your-digital-trails-polices-hands/ (describing law enforcement's use of "geofence warrants" and "keyword warrants" to request location and search history data from private companies); David Uberti, *Police Requests for Google Histories Face New Scrutiny*, Wall St. J. (July 27, 2020, 5:30 AM), https://www.wsj.com/articles/police-requests-for-google-users-location-histories-face-new-scrutiny-11595842201 (same).

2 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1107 (2002) ("The government can increasingly amass vast dossiers on millions of individuals . . . without any probable cause or particularized suspicion.").

3 *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Automated License Plate Readers (ALPRs), Elec. Frontier Found. (Aug. 28, 2017), https://www.eff.org/pages/automated-license-plate-readers-alpr (describing ALPR technology and its law enforcement uses).

4 *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. Rev. 1827, 1871–72 (2015).

5 *See* Elizabeth E. Joh, Essay, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 Wash. L. Rev. 35, 48–50, 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").

6 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 (discussing law enforcement's use of genetic genealogy technology and open-source DNA platforms to apprehend the Golden State Killer).

7 *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://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy.

8 There were early reports that location-based predictive policing had value. *See* Stuart Wolpert, *Predictive Policing Substantial Reduces Crime in LA*, UCLA Newsroom (Oct. 7, 2015), https://newsroom.ucla.edu/releases/predictive-policing-substantially-reduces-crime-in-los-angeles-during-months-long-test (discussing LAPD's successful use of predictive policing to combat crime). But the LAPD has discontinued the use of these algorithms because of uncertain value and evidence of social costs. *See* Mark P. Smith, Inspector Gen., L.A. Police Comm'n, Review of Selected Los Angeles Police Department Data-Driven Policing Strategies 3–6, 24–25 (2019), https://a27e0481-a3d0-44b8-8142-1376cfbb6e32.filesusr.com/ugd/b2dd23_21f6fe20f1b84c179abf440d4c049219.pdf (discussing significant errors present in LAPD's "operation LASER," a data-focused crime prevention program aimed at individuals most likely to commit crime). Person-based predictive policing has proven a bust. *See* Jeremy Gorner & Annie Sweeney, *For Years Chicago Police Rated the Risk of Tens of Thousands Being Caught Up in Violence. That Controversial Effort Has Quietly Been Ended*, Chi. Trib. (Jan. 24, 2020, 8:55 PM), https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html (discussing recently scrapped Chicago Police Department program, which used data gathering to predict those individuals who are most likely to be victims and perpetrators of crime).

9 *See* Barry Friedman, *Lawless Surveillance* (unpublished manuscript) (on file with author); Danielle Citron and Barry Friedman, *Policing Private Data Collection* (unpublished manuscript) (on file with author).

10 FBI, *Next Generation Identification (NGI)*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Aug. 30, 2021, 7:15 PM); *FBI's Next Generation Identification Biometrics Database*, Elec. Frontier Found., https://www.eff.org/cases/fbis-next-generation-identification-biometrics-database; (last visited Aug. 30, 2021, 7:15 PM).

11 *See* Ángel Díaz, Brennan Ctr. for Just., *New York City Police Department Surveillance Technology* (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology (describing technology used by NYPD, including its Domain Awareness system).

12 *See* Elizabeth E. Joh, Essay, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. U. L. Rev. 857, 860–62 (2006) (describing local DNA databases and techniques by which police have gathered or tricked suspects into providing DNA including by retrieving a used coffee cup or having them lick an envelope).

13 *See* Logan Koepke et al., Upturn, Mass Extraction 4–11 (2020), https://www.upturn.org/reports/2020/mass-extraction (documenting the widespread adoption of Cellebrite and other Mobile Device Forensic Tools by law enforcement).

14 *Thomson Reuters CLEAR*, Thomson Reuters Legal, https://legal.thomsonreuters.com/en/c/clear-investigation-solution (last visited Aug. 30, 2021).

15 *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.

16 Sam Biddle, *LexisNexis to Provide Giant Database of Personal Information to ICE*, Intercept (Apr. 2, 2021, 10:00 AM), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis.

17 AI Ethics Board, Axon, *Second Report of the Axon AI & Policing Technology Ethics Board: Automated License Plate Readers* 5, 12 (2019); https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf.

18 See *id.* at 13; Christopher S. Koper & Cynthia Lum, *The Impacts of Large-Scale License Plate Reader Deployments on Criminal Investigations*, 22(3) Police Q. 305, 309, 321 (2019); 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.

19 *See* AI Ethics Board, *supra* note 17, at 13–14 (discussing how technological advancements and private competition decreased costs of ALPRs and encouraged their additional use).

20 *See Axon Fleet 3 Has Arrived*, Axon (June 30, 2021), https://www.multivu.com/players/English/8829452-axon-fleet-3-video-system-alpr-shipping-public-safety-agencies; *Axon Fleet 3 and Automatic License Plate Recognition (ALPR) Frequently Asked Questions*, myAxon, https://my.axon.com/s/article/Fleet3-ALPR-FAQs?language=en_US (last visited Aug. 30, 2021).

21 Auditor of the State of Cal., Rep. No. 2019–118, Automated License Plate Readers 12, 29 (2020), https://www.auditor.ca.gov/reports/2019-118/summary.html.

22 Myrtle Beach City Government, Facebook (Feb. 29, 2020), https://www.facebook.com/myrtlebeachcitygovernment/posts/2697108117183824.

23 *See* Joseph Cox, *This Company Built a Private Surveillance Network. We Tracked Someone with It*, Vice (Sept. 17, 2019, 10:45 AM), https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn; Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police for Deportations*, ACLU: Blog (Mar. 13, 2019, 11:00 AM), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data (discussing contracts between law enforcement and Vigilant for access to the company's massive ALPR database).

24 *See* Justin Jouvenal et al., *Data on a Genealogy Site Led Police to the "Golden State Killer" Suspect. Now Others Worry About a "Treasure Trove of Data,"* Wash. Post (April 27, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/04/27/data-on-a-genealogy-site-led-police-to-the-golden-state-killer-suspect-now-others-worry-about-a-treasure-trove-of-data.

25 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.

26 Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (Aug. 30, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

27 *See* Mark Puente & Richard Winton, *L.A. Vows To Void 2 Million Court Citations and Warrants. Homeless People Will Benefit Most*, L.A. Times (Oct. 2, 2019, 5:02 PM), https://www.latimes.com/california/story/2019-10-02/homeless-housing-erase-citation-fine-fees (noting how the Los Angeles County district attorney sought to void

248,000 county warrants and roughly 900,000 infraction citations—more than half of which were older than ten years); Beth Fertig, *City District Attorneys Purge Almost 645,000 Old Warrants*, WNYC (Aug. 9, 2017), https://www.wnyc.org/story/city-district-attorneys-purge-645000-old-warrants (discussing how New York City district attorneys sought to dismiss almost 645,000 warrants, all of which were over ten years old).

28 Off. of the Legis. Auditor, State of Minn., Law Enforcement's Use of State Databases 26 (2013), https://www.auditor.leg.state.mn.us/ped/pedrep/ledatabase.pdf.

29 *See* Sadie Gurman, *AP: Across US, Police Officers Abuse Confidential Databases*, AP News (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43?utm_campaign=socialflow&utm_source=twitter&utm_medium=ap (explaining misuse of law enforcement databases frequently related to officers snooping on romantic partners and describing multiple examples of how officers have used information to stalk and harass women).

30 *See, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 104–05 (2008) (arguing that Fourth Amendment case law should refocus on guaranteeing a right to security over a right to privacy); Benjamin Wittes, Brookings Inst., *Databuse: Digital Privacy and the Mosaic* 15 (2011), https://www.brookings.edu/wp-content/uploads/2016/06/0401_databuse_wittes.pdf (discussing how one of the greatest harms of privacy breaches are personal security concerns); 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, 296 (2021) (explaining how policing has threatened the security of Black Americans violating the Fourth Amendment's promise of personal security for all); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 Stan. L. Rev. 1039, 1050 n. 33 (2016) (citing wealth of sources urging focus on "security").

31 *See* Amna Toor, Note, *"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, 295–97 (2018) (discussing how in addition to surveilling civil rights groups, the FBI also sought to discredit their leaders and disrupt their recruitment efforts).

32 *See* 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, including legitimate candidates for office and Catholic nuns); Will Parrish & Jason Wilson, *Revealed: Anti-Terror Center Helped Police Track Environmental Activists*, Guardian (Oct. 2, 2019, 2:00 PM), https://www.theguardian.com/us-news/2019/oct/02/oregon-pipelines-protests-monitoring-police-anti-terror-unit (describing how the Oregon Titan Fusion Center monitored groups protesting a fossil fuel project in the state and supporters of the Black Lives Matter movement).

33 Barton Gellman & Sam Adler-Bell, *The Century Foundation, The Disparate Impact of Surveillance* 5–6 (2017); Rachel Levinson-Waldman, *Why the Surveillance State is Everybody's Problem*; Brennan Ctr. (May 12, 2015), https://www.brennancenter.org/our-work/analysis-opinion/why-surveillance-state-everybodys-problem.

34 *See* Automated License Plate Readers (ALPRs), *supra* note 3 (discussing how in New York, Birmingham, and Oakland police targeted ALPR surveillance against communities of color); Toor, *supra* note 31, at 294–301 (tracing the long history of government surveillance of Black communities through today).

35 *See, e.g.*, Gregory Brazeal, *Mass Seizure and Mass Search*, 22 U. Pa. J. Const. L. 1001, 1003 (2020) ("[T]he Fourth Amendment . . . currently provides no protection against the vast majority of existing and possible forms of digital mass surveillance.").

36 Wittes, *supra* note 30, at 12 (footnote omitted).

37 Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 Kan. L. Rev. 485, 488 (2018).

38 United States v. Jacobsen, 466 U.S. 109, 113 (1984) (quoting Walter v. United States, 447 U.S. 649, 662 [1980] [Blackmun, J., dissenting]).

39 *See* Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 19 (2008) ("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. But courts 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." [footnote omitted]).

40 Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citing Kyllo v. United States, 533 U.S. 27, 34 [2001]).

41 *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.'"); Christopher Slobogin, *Transaction Surveillance by the Government*, 75 Miss. L.J. 139, 152 (2005) ("The Fourth Amendment's justification requirements—probable cause and the like—only apply if government engages in a 'search or seizure.'").

42 *See* Katz v. United States, 389 U.S. 347, 351 (1967) (holding that people had no "reasonable expectation of privacy" in what they "knowingly exposed" to the public).

43 United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

44 *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 and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

45 United States v. Jones, 565 U.S. 400, 404 (2012), https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

46 *Id.* at 430 (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."); *id.* at 416 (Sotomayor, J., concurring).

47 Carpenter v. United States, 138 S. Ct. 2206, 2212, 2219 (2018).

48 *Id.* at 2223–24 (Kennedy, J., dissenting).

49 *Id.* at 2219 (majority opinion).

50 *Id.* at 2018.

51 *Id.*

52 *Id.*

53 *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").

54 *See generally* Barry Friedman & Elizabeth G. Jánszky, *Policing's Information Problem*, 99 Tex. L. Rev. 1 (2020) (offering public choice theory as an explanation for legislative inaction around policing though questioning why this is so); 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).

55 *See generally* Bart Forsyth, *Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection*, 72 Wash. & Lee L. Rev. 1307 (2015) (discussing the passage of the USA FREEDOM Act and its effect on bulk government data collection).

56 388 U.S. 41 (1967).

57 389 U.S. 347 (1967).

58 *See* Patricia L. Bellia, Feature, *Federalization in Information Privacy Law*, 118 Yale L.J. 868, 879 (2009) (describing how the Federal Wiretap Act was Congress' response to the Fourth Amendment requirements the Court identified in *Katz* and *Berger*).

59 *See generally* Meghan Holloway, Comment, *Penalty Default Rules for Digital Searches: Why Courts Should Spur Legislative Action via Second-Order Regulation*, 87 U. Chi. L. Rev. 1395 (2020) (arguing that courts should institute penalty default rules that disadvantage the police to incentivize legislatures to regulate digital searches); John Ferejohn & Barry Friedman, *Toward a Political Theory of Constitutional Default Rules*, 33 Fla. St. U. L Rev. 825 (2006).

60 *See* Barry Friedman, *Lawless Surveillance* (unpublished manuscript) (on file with author) (detailing how three Fourth Amendment doctrines—searches, seizures, and special needs searches, the Fifth Amendment, and the Fourteenth Amendment's Due Process and privacy rights can support requiring regulation of bulk data collection).

61 *See* Boyd v. United States, 116 U.S. 616, 634–35 (1886).

62 *Id.* at 627–28 (quoting Entick v. Carrington [1765] 95 Eng. Rep. 807 [KB]).

63 *Id.* at 630.

64 Hale v. Henkel, 201 U.S. 43 (1906).

65 *Id.* at 73.

66 *Id.* at 76.

67 Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946).

68 *Id.*

69 *Id.*

70 *Id.*

71 Craib v. Bulmash, 777 P.2d 1120, 1124 (1989) (citing *Oklahoma Press*, 327 U.S. at 209) (holding that under the Fourth Amendment, administrative subpoenas may only be issued for "a *lawfully authorized purpose*, within the power of [the legislative body] to command" and noting that *Oklahoma Press* is "the leading case" on the matter [alteration in original]).

72 FTC v. Am. Tobacco Co., 264 U.S. 298 (1924).

73 *Id.* at 306.

74 *Oklahoma Press*, 327 U.S. at 207 (citing *Am. Tobacco Co.*, 264 U.S. at 305).

75 United States v. Theodore, 479 F.2d 749, 754–55 (4th Cir. 1973).

76 *Id.* at 754.

77 *Id.*

78 Resolution Trust Corp. v. Walde, 18 F.3d 943, 947 (D.C. Cir. 1994).

79 *Id.* at 949.

80 McVane v. FDIC, 44 F.3d 1127, 1135 (2nd Cir. 1995) (quoting *Walde*, 18 F.3d at 946).

81 *Id.* at 1138.

82 *Id.* (quoting Fed. Elec. Comm'n v. Larouche Campaign, 817 F.2d 233, 234 [2d Cir. 1987] [per curiam])

83 United States v. Powell, 379 U.S. 48, 58 (1964) (quoting Reisman v. Caplin, 375 U.S. 440, 449 [1963]).

84 335 U.S. 1, 3–4 (1948).

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

86 *Id.* at 51 (Frankfurter, J., dissenting).

87 390 U.S. 39 (1968).

88 *Id.* at 57.

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

90 *Id.* at 27.

91 *Id.* at 26.

92 *Id.* at 32.

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

94 Marchetti v. United States, 390 U.S. 39, 57 (1968) (quoting Albertson v. Subversive Activities Control Bd., 382 U.S. 70, 79 [1965]).

95 Grosso v. United States, 390 U.S. 62, 67–68 (1968).

96 *Id.* at 68.

97 United States v. Westinghouse Elec. Corp., 638 F.2d 570, 576 (3d Cir. 1980) (quoting Olmstead v. United States, 277 U.S. 438, 478 [1928] [Brandeis, J., dissenting]).

98 Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

99 Whalen v. Roe, 429 U.S. 589, 591–94 (1977).

100 *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 433–36 (1977) (discussing statute in question).

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

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

103 *Id.* at 456 (quoting Nixon v. Adm'r of Gen. Servs., 408 F. Supp 321 [1976]).

104 *Whalen*, 429 U.S. at 597; *see id.* at. 597–98.

105 *Id.* at 597.

106 *Id.* at 598.

107 *Id.* at 597.

108 *Id.* at 598.

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

110 United States v. Westinghouse Elec. Corp., 638 F.2d 570, 580 (3d Cir. 1980).

111 *Id.* at 581.

112 *Whalen*, 429 U.S at 605.

113 *Id.* at 606 (majority opinion); *see also id.* at 606–07 (Brennan, J., concurring).

114 *See, e.g.*, NAACP v. Alabama ex rel., Patterson, 357 U.S. 449, 466 (1958) (holding that Alabama's requirement that the NAACP disclose its membership lists unconstitutionally infringed on the NAACP's right to association); Ams. for Prosperity Found. v. Bonta, 141 S. Ct. 2373, 2389 (2021) (same; California regulation requiring donor disclosure information from nonprofits); Heller v. District of Columbia, 801 F.3d 264 (D.C. Cir. 2015) (holding that D.C.'s requirement for information as part of firearm registration did not violate the Second Amendment).

115 *See* Balkin, *supra* note 39, at 12 ("We leave traces of ourselves continually, including our location, our communications contacts, our consumption choices—even our DNA."); 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.")

116 *See supra* note 60 and accompanying text.

117 *See* 533 U.S. 27, 34–40 (2001).

118 *See* New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

119 *See, e.g.*, Griffin v. Wisconsin, 483 U.S. 868, 873, 880 (1987); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–54 (1995); Ferguson v. City of Charleston, 532 U.S. 67, 74–76 (2001).

120 *See, e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 449–55 (1990) (sobriety checkpoints); Treasury Employs. v. Von Raab, 489 U.S. 656, 675 n.3 (1997) (referring to airport security).

121 *Acton*, 515 U.S. at 652–53.

122 *See, e.g.*, Donovan v. Dewey, 452 U.S. 594, 603 (1981) ("[T]he statute's inspection program, in terms of the certainty and regularity of its application, [must] provid[e] a constitutionally adequate substitute for a warrant."); New York v. Burger, 482 U.S. 691, 703 (1987) (quoting *Dewey*, 452 U.S. at 600) (same); 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. . . .'" [footnote omitted] [first quoting United States v. Martinez-Fuerte, 428 U.S. 543 (1976), then quoting Camara v. Mun. Ct., 387 U.S. 523, 532 (1967)]).

123 *See, e.g.*, Camara v. San Francisco, 387 U.S. 523, 538 (1967) (requiring that "reasonable legislative or administrative standards . . . are satisfied" prior to conducting municipal health and safety inspections); United States v. Biswell, 406 U.S. 311, 315 (1972) ("In the context of a regulatory inspection system of business premises . . . the legality of the search depends not on consent but on the authority of a valid statute.").

124 *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified as amended in scattered sections of 18 and 50 U.S.C.); Forsyth, *supra* note 55 and accompanying text.

125 *See* Forsyth, *supra* note 55, at 1338–39 ("[T]he government [must] demonstrate a reasonable, articulable suspicion that a specific selection term is associated with . . . international terrorism, [before] the FISC may issue an order for the ongoing, daily production of call detail records held by telephone companies." [footnote omitted]).

126 *See* Friedman & Ponomarenko, *supra* note 4, at 1184 (discussing how policing agencies are typically authorized by "statutes of sweeping generality, typically adopted some time ago").

hoover.org

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Barry Friedman, *Private Data/Public Regulation*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2105 (October 4, 2021), available at https://www.lawfareblog.com/private-datapublic-regulation.

About the Author

BARRY FRIEDMAN

Professor Friedman is the Jacob D. Fuchsberg Professor of Law and Affiliated Professor of Politics at New York University's School of Law and the founding director of the school's Policing Project. He is the author of *Unwarranted: Policing with Permission* and many academic articles in law, politics, and history. He also publishes regularly in the popular media.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION