2017

When Database Queries Are Fourth Amendment Searches

Emily Berman

Article

When Database Queries Are Fourth Amendment Searches

Emily Berman†

INTRODUCTION

As anyone familiar with *Law & Order* knows, the Fourth Amendment demands that—before conducting a search or seizure—the government must secure a warrant. To be valid, the warrant must (1) be approved by a neutral decision-maker; (2) be based on a showing of probable cause; and (3) describe with particularity the places to be searched or the things to be seized.[1]

Outside the world of police procedurals, however, the legal framework regulating the government's investigative powers permits the collection of a great deal of information without abiding by prior approval, individualized cause,[2] or particularity requirements. Specifically, investigators need not meet traditional warrant requirements in at least two types of situations—warrant requirement exceptions and what I call "Fourth Amendment exemptions."[3] When an exception to the warrant requirement applies, the government satisfies Fourth Amendment demands merely by demonstrating that its actions are

† Assistant Professor of Law, University of Houston Law Center. Thanks go to Seth Chandler, Dave Fagundes, Barry Friedman, Aziz Huq, David Kwok, James Nelson, D. Theodore Rave, Jessica Roberts, Joe Sanders, and Greg Vetter, as well as participants in the 2016 Texas Legal Scholars workshop, the 2017 AALS National Security Law Section's New Voices Panel, and the 2017 Michigan Young Scholars Conference, particularly Peter Margulies, Dakota Rudesill, and Margo Schlanger. All errors are the author's.

1. FED. R. CRIM. P. 41.

2. An "individualized suspicion" requirement demands that the government show cause—usually probable cause or reasonable suspicion—to believe that a search of a *particular* individual is justified. United States v. Chandler, 520 U.S. 305, 305–06 (1997).

3. *See infra* Part II.A.1.

reasonable.[4] In Fourth Amendment exemptions, the government's collection activity does not violate a reasonable expectation of privacy and therefore the Fourth Amendment does not regulate the collection at all.[5] Such investigative activity is considered neither a search nor a seizure, and is thus exempt from constitutional limitations. Together, warrant requirement exceptions and Fourth Amendment exemptions permit the government to lawfully scoop up an enormous volume of information about Americans, often without any reason to suspect any particular American of wrongdoing and with no demonstrated connection to crime or specific intelligence needs.

Moreover, there are no constitutional restrictions at all on how the government uses this vast expanse of data. So long as its collection is lawful, the Fourth Amendment has nothing to say about how information is employed.[6] Rather, current constitutional doctrine allows the government to combine, compile, and analyze any information in its possession—even as the volume of this information becomes ever larger and analytical tools ever more powerful.

Courts and commentators recognize that the government's broad collection authority raises significant privacy concerns. The conventional response is to suggest expanding the scope of collection regulation, either by narrowing warrant requirement exceptions[7] or broadening the definition of what qualifies as a search or seizure.[8] Thus existing doctrine and extant reform

4. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 126–27 (2000) (discussing the court's analysis of reasonable suspicion).

5. Katz v. United States, 389 U.S. 347 (1967). The reasonable-expectation-of-privacy inquiry asks first whether the government has violated an expectation of privacy, and second, whether society is prepared to accept that expectation as reasonable. *Id.* at 360 (Harlan, J., concurring); *see also infra* notes 77–80 and accompanying text.

6. *See infra* Part II.B.

7. *E.g.*, BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION (2017) (discussing policing reform in the United States).

8. The most common suggestion is to eliminate or constrain the third-party doctrine, which exempts from Fourth Amendment protections any information voluntarily conveyed to a third party. *See, e.g.*, Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1252–53 (2009) (arguing that the third-party doctrine's application should vary based on the voluntariness with which the records were shared); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 249–50 (2015) (arguing that the government should be required to obtain a warrant prior to seizing some third-party data); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1157 (2002) [hereinafter Solove, *Digital Dossiers*] (arguing that the

proposals both accept as given that the Fourth Amendment's scope is limited to regulation of information collection. The privacy impact of large amounts of data, however, does not come solely from the sweeping nature of the government's *collection* authority. The government's postcollection *use* of information can—and often does—implicate privacy interests just as strongly.

This Article focuses on one form of information use with particularly troubling effects on privacy: database queries that implicate the aggregation problem.[9] The aggregation problem, a label coined by Professor Daniel Solove, refers to the fact that the government can collect enough data—both in the sense of volume and of variety—that its aggregation and analysis can actually change the nature of the information, providing revelations that could not have been gleaned from the isolated bits of information alone.[10] At a certain point, the whole equals more than the sum of its parts. Yet because such aggregation necessarily takes place only after the information is collected, the extraction of such revelations is not subject to any constitutional restrictions. I contend that when database queries about particular U.S. persons have the capacity to aggregate data such that it will reveal information that, in the absence of aggregation, the government could only access by conducting a search or seizure, the extraction of that information should be subject to constitutionally based limits.[11] In other words, when

third-party doctrine should apply only to "systems of records"); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (arguing that the third-party doctrine does not apply to bulk collection of telephony metadata). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (defending the third-party doctrine).

9. Solove, *Digital Dossiers*, *supra* note 8, at 1154.

10. *Id.*; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 514 (2006) [hereinafter Solove, *A Taxonomy of Privacy*] ("Aggregation creates . . . a 'digital person,' a portrait composed of information fragments combined together."); *see also* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105, 110 (2000) (noting that "two (conventional) data about an individual, each innocuous in itself" can together "produce new (conventional) knowledge about the individual").

11. Database queries about particular U.S. persons are distinct from what is commonly labeled data mining. *See infra* notes 157–58 and accompanying text. This Article's analysis is limited to U.S. person queries and leaves discussion of Fourth Amendment limits on data mining to future work. Indeed, there is already a vibrant and quickly growing literature regarding the constitutional implications of data mining. *E.g.*, Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461 (2015) (discussing trends in policing technique); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L.

a database query returns information that the government could otherwise collect only through a Fourth Amendment–regulated means, the Fourth Amendment should regulate that query. If the government accesses an American's electronic communications, for example, the same expectation of privacy is violated—the expectation that the government does not have access to our private communications in the absence of a court order[12]—regardless of whether the government collected those communications directly, pursuant to a warrant, or accessed them by querying a database in which communications collected incidentally to the targeting of a non-American are stored.[13] Note that the Constitution is triggered here by the nature of the information *exposed* by the query, not the nature of the information that makes up the underlying database(s).[14]

The Fourth Amendment should regulate information *use* as well as its *collection*, I argue, because no modification to the collection rules will address threats to privacy that come solely from information use.[15] The digital age has rendered collection-focused efforts alone an insufficient means of preserving individual privacy, particularly in light of the fact that the government (1) is able to extract more information from the same data

REV. 327, 329–30 (2015) (discussing current trends toward "big data" and away from "small data"); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 265 (2012) (analyzing possible effect of data analysis on policing); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014); Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 812 (2010) (discussing the impact of databases on law enforcement).

12. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972) (so holding in the intelligence context); Berger v. New York, 388 U.S. 41 (1967) (so holding in the criminal context).

13. The reasonable-expectation-of-privacy test itself is generally recognized to be unpredictable and largely circular. *See infra* notes 159–61 and accompanying text. But so long as *Katz* governs the question of what qualifies as a search, that is the relevant standard. Moreover, to the extent that queries expose knowledge, the collection of which is already definitively recognized as a search, the indeterminate nature of the *Katz* inquiry itself does not pose a problem.

14. Recognizing a reasonable expectation of privacy in a database search is concededly a significant expansion of *Katz's* reasonable expectation of privacy test, which to date has applied only to information collection. This expansion, however, is no more significant than the expansion of Fourth Amendment coverage that *Katz* itself represented at the time. *See infra* notes 187–93 and accompanying text.

15. This is not to say that collection reforms are not also important. I agree, for example, that the third-party doctrine should be curtailed. The point here is simply that if the concern comes from how the government is using information, reforming collection rules cannot alleviate that concern entirely.

than it used to;[16] and (2) that the costs of storage and analysis have plummeted.[17]

Of course, the Constitution is not the only source of legal restrictions on government activity. Statutory, regulatory, policy-based, or judicially imposed constraints apply to use at times. Exactly what rules govern the collection and use of particular types of information vary, depending on both the nature of the data and the nature of the collection. When it comes to data regarding electronic communications, for example, noncontent data (or metadata)—like call records or email routing information—currently lacks constitutional protection.[18] But that data is subject to statutory constraints on its collection.[19] The same is true for data such as financial and medical records. Even information that normally enjoys full Fourth Amendment protection under the warrant requirement, such as electronic communications, can sometimes be subject to a different regime. Thus when collecting electronic communications by targeting non-U.S. persons outside the United States for foreign intelligence purposes, which will inevitably collect the communications of U.S. persons as well—that collection need only be reasonable to satisfy the Constitution,[20] while more specific regulation comes from other sources.[21] A patchwork of limits from disparate sources regulates the vast sea of data unrelated

16. Blood collected at a crime scene, for example, historically could only allow law enforcement to determine its type. Now that same sample can provide a detailed genetic profile. Sophisticated analysis of large volumes of data has similarly magnified the volume of knowledge that can be extracted from information. *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008) (discussing the expansion of the government's ability to analyze data about American citizens).

17. *See* United States v. Jones, 565 U.S. 400 (2012) (noting that technological advances enable greater police surveillance).

18. *See In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED] 9 (FISA Ct., Aug. 29, 2013) (holding that collection of bulk telephony metadata is not regulated by the Fourth Amendment).

19. *See* 50 U.S.C. § 1842(h)(1) (2012) (instructing the Attorney General to develop "appropriate policies and procedures" for protecting the privacy of "nonpublicly available information concerning United States persons"); USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 201–202, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861) (prohibiting bulk collection and instituting privacy procedures).

20. *In re* Directives [REDACTED] Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

21. *See infra* notes 107–11 and accompanying text (discussing the nonconstitutional limits on government use of Americans' electronic communications captured in the courts of foreign intelligence surveillance).

to communications—social media postings; digital records of an individual's movements; and public records such as arrests, real estate purchases, or professional licenses.

Some commentators argue that these unconstitutional rules are the appropriate means to regulate the government's use of information.[22] I disagree for a number of reasons.[23] First, if limits on information collection are any guide, nonconstitutional restrictions are often significantly less protective than Fourth Amendment–based regulation, frequently requiring only that the information is relevant to an ongoing investigation.[24] Second, Congress has been an unreliable actor in this area, legislating piecemeal—often in response to some form of scandal—rather than developing a comprehensive information privacy regime.[25] Similarly, internal or executive branch policy constraints generate a hodgepodge of rules, with different regulations applicable to different agencies, any of which may be modified at any time and are frequently secret. These are not qualities that generate sustained, meaningful privacy protections. Finally, the government is now capable of uncovering many of our most intimate details—things that historically might have been discoverable only by searching someone's "papers"[26]—simply by manipulating data. Fourth Amendment doctrine must evolve to recognize some database queries as searches just as it has evolved over time in other ways to ad-

22. *See, e.g.*, Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, *in* THE FUTURE OF THE CONSTITUTION 3 (2011) (advocating for regulation of the entire surveillance process); William C. Banks, *Programmatic Surveillance and FISA: Of Needles and Haystacks*, 88 TEX. L. REV. 1633, 1637 (2010) (arguing for the development of a standardized system for authorized use of collected information); Solove, *A Taxonomy of Privacy*, *supra* note 10, at 521–22 (describing a framework through which to understand privacy). *But see*, Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C.L. REV. (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937809 (reviewing use restrictions and discussing their justifications).

23. *See infra* Part III.C (discussing the need for constitutional regulation).

24. *See, e.g.*, Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 149–67 (2005) (detailing the ease with which the government may collect call detail records, public records, medical records, credit information, stored communications, tangible things, and more); *see also infra* notes 251–52.

25. *See infra* notes 253–61 and accompanying text (discussing the insufficiency of legislative action).

26. The Fourth Amendment protects from unreasonable searches and seizures of people's "persons, houses, papers, and effects." U.S. CONST. amend. IV.

dress challenges posed by new technology and new investigative techniques.[27]

While my proposal would significantly expand the Fourth Amendment and may sound drastic, it is not as stark a divergence from existing doctrine as it may first appear. Indeed, my doctrinal approach builds on two existing strands of Fourth Amendment law. The first is a series of what I call collection-plus situations—circumstances in which collection is constitutionally permissible only when *paired* with postcollection use restrictions.[28] The Supreme Court has determined, for example, that foreign intelligence surveillance is consistent with the Fourth Amendment only when exercised in concert with "minimization procedures"—rules governing the government's retention and dissemination of the fruits of that surveillance.[29] Imposing constitutional constraints on information use alone—as opposed to imposing them in conjunction with limits on particularly intrusive collection techniques—merely takes an additional step down that path.

The other strand of Fourth Amendment law on which I draw comes from the Supreme Court's recent efforts to grapple with the powerful effects of information aggregation. *United States v. Jones* examined the scope of the government's authority to engage in long-term warrantless GPS tracking. Black letter Fourth Amendment law provides that information identifying one's location in a public space at any given moment is exempt from Fourth Amendment protection.[30] In *Jones*, however, the Court faced the question whether aggregating information about an individual's precise location over the course of several weeks should lie similarly beyond the Constitution's reach. In concurring opinions, five justices agreed that because such a "precise, comprehensive record of a person's public movements" exposes "a wealth of detail about [that person's] familial, political, professional, religious, and sexual associations," it violates a reasonable expectation of privacy and should therefore be considered a search.[31] In other words, the

27. *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (discussing how courts adjust Fourth Amendment doctrine in response to technology).

28. *See infra* notes 204–17 and accompanying text.

29. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 321 (1972); Berger v. New York, 388 U.S. 41, 58 (1967).

30. *See infra* notes 93–96 and accompanying text.

31. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *see, e.g.*, Riley v. California, 134 S. Ct. 2473, 2492 (2014) (rejecting

aggregation of many pieces of data was simply too intrusive to go unregulated, even though the collection of any one piece of that data—the defendant's location at any given moment—remained untouched by Fourth Amendment limits. When database queries about U.S. persons similarly reveal intimate knowledge discoverable only by aggregating multiple pieces of data, courts should consider those queries Fourth Amendment searches, regardless of how the data were collected.

Any objections to my proposal based on logistical concerns fail as well. The Foreign Intelligence Surveillance Court (FISC) has already provided a model for implementing these doctrinal changes in its own jurisprudence.[32] As I have argued elsewhere, the FISC imposed constraints in the form of minimization procedures on the government's Section 215 bulk telephony metadata program that approximated each of the Fourth Amendment warrant requirement's elements.[33] And while the FISC did not explicitly rest these restrictions on constitutional foundations, its means of imposing ex ante review, as well as cause and particularity requirements, nevertheless provides a blueprint for what a Fourth Amendment use-restriction regime might look like.

This Article will proceed in three parts. Part I will first illustrate the incredible breadth and volume of information the government may collect. It will then demonstrate the threat to privacy that the power to aggregate that data poses. Part II turns to Fourth Amendment doctrine, first explaining how warrant requirement exceptions and Fourth Amendment exemptions remove much information collection from constraints traditionally applicable to searches and seizures and then exploring the powerful investigative tool this collection represents in light of the absence of use restrictions. In Part III, I will begin by making the case for treating as searches some database queries about U.S. persons. I will then show how the FISC's jurisprudence provides a model for how this doctrinal shift might be implemented. Finally, I will explain why we

the warrantless search of an arrestee's cell phone given the nature of the revelations made possible by searching smartphone contents); *see also Jones*, 565 U.S. at 419–31 (Alito, J., concurring).

32. The Foreign Intelligence Surveillance Court (FISC) is a federal court created by the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801–1885(c) (2012) to review government applications to engage in domestic surveillance for foreign intelligence purposes. *Id.* § 1803(d).

33. Emily Berman, *Quasi-Constitutional Protections and Government Surveillance*, 2016 B.Y.U. L. REV. 771 (2016).

need constitutionally based use restrictions, rather than relying on statutory or regulatory rules. The Article will then briefly conclude.

I. COLLECTION AND AGGREGATION OF INFORMATION

This Part surveys the types of information the government collects about Americans and demonstrates that when the volume and variety of this information is combined with the government's analytical capacity "it is possible to learn far more than most people had anticipated."[34]

A. THE INFORMATION THE GOVERNMENT CAN COLLECT[35]

Most information the government collects does not implicate the Fourth Amendment at all. Information regarding immigration, social security benefits, military service, census information, and income tax is collected and stored in the course of everyday operations. Other sources of information are government audits, agency oversight activities, personnel hiring, and more. Many of these records will include information such as an individual's physical description, family history (marriages, divorces, children), place of residence, political activity, financial information, health care records (including medical conditions and use of prescription drugs), social security number, and beyond.[36] Statutes and regulations—rather than constitutional law—control government access to this type of information.

Of course, intelligence and law enforcement operations also engage in their own major collection operations. We learned with great fanfare in 2013 from the Edward Snowden leaks that the National Security Agency (NSA) had been collecting since 2006, bulk telephony metadata records—comprised of in-

34. John P. Holdren & Eric S. Lander, *Letter to President Barack Obama*, *in* BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014). One hint at the volume of information involved comes from the NSA's recent construction of a data storage facility roughly five times larger than the U.S. Capitol. James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), https://www.wired.com/2012/03/ff_nsadatacenter.

35. As this path has been well-trodden by others, this discussion will provide a broad overview. For more detailed discussion about government information collection, I commend to you the sources cited in notes 36–52, *infra*.

36. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002) [hereinafter Solove, *Access and Aggregation*].

formation such the length of a call, the phone number from which the call was made, and the phone number dialed—produced by each telephone company regarding "all telephone calls made through its systems or using its services where one or both ends of the call are located in the United States."[37] The revelation that, going back as far as 1987, the Drug Enforcement Administration (DEA) had "routine access" to similar information regarding "every call that passes through an AT&T switch—not just those made by AT&T customers"—drew less attention.[38] Call detail records are available to the government if they are "relevant and material to an ongoing criminal investigation."[39] Law enforcement entities regularly seek other information from communications providers as well, notably cell site location information.[40] The Supreme Court granted certio-

37. ACLU v. Clapper, 785 F.3d 787, 796 (2d Cir. 2015). "Metadata can also reveal the user or device making or receiving a call through unique 'identity numbers,'" as well as the routing of a call, which can indicate a caller's general location. *Id.* at 793–94; *see also* ADMIN. WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 3 (2013) (explaining the government's legal basis for an intelligence collection program). Defining the line between content and metadata in the context of electronic communications has proved less than straightforward. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that e-mails constitute communications content protected by the Fourth Amendment); United States v. Forrester, 512 F.3d 500 (9th Cir. 2007) (finding that Internet Protocol addresses are noncontent metadata).

38. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES (Sept. 1, 2013), http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

39. 18 U.S.C. § 2703(d) (2012).

40. Cell site location information (CSLI) is the compilation of data that cellular phones communicate with cell towers, conveying to cellular service providers details regarding the tower locations relied upon by users. According to AT&T, that company received 64,703 requests for such information in 2014; in the first half of 2015, Verizon received more than 21,000 such requests. Robinson Meyer, *Do Police Need a Warrant To See Where a Phone Is?*, ATLANTIC (Aug. 8, 2015), https://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775. For readers familiar with the podcast *Serial*, you may recall that much of the government's case against Adnan Syed for the 1999 murder of Hae Min Lee came from CSLI, and much of the uncertainty regarding his guilt or innocence comes from debate regarding the accuracy and reliability of such records. *See Season One*, SERIAL, https://serialpodcast.org/season-one (last visited Nov. 5, 2017). For readers unfamiliar with *Serial*, do yourself a favor and listen to season one as soon as possible. Several circuits have determined that acquiring an individual's historical CSLI is not a search and therefore does not require a warrant. *See, e.g.*, United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

rari this Term to decide whether the warrantless collection of this kind of location information enjoys Fourth Amendment protection.[41]

Police forces and the FBI have an insatiable desire for data, and deploy a variety of sophisticated information collection tools to acquire it: cell tower simulators,[42] automatic license-plate-recognition cameras—a technology designed to mark the location of a particular vehicle at a particular time[43]—and a variety of surveillance cameras mounted on aerial drones,[44] in fixed locations, and on police cars and police officers.[45] Sophisticated means of conducting covert audio, video, and tracking surveillance are marketed to cities flush with counterterrorism funding.[46] The New York Police Department (NYPD) has

41. Carpenter v. United States, 137 S. Ct. 2211 (2017).

42. *See, e.g.*, Nicky Woolf, *Stingray Documents Offer Rare Insight into Police and FBI Surveillance*, GUARDIAN (Aug. 26, 2016), http://www.theguardian.com/us-news/2016/aug/26/stingray-oakland-police-fbi-surveillance (discussing the FBI's use of cell site simulators).

43. *See* Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, ARS TECHNICA (Sept. 27, 2012), https://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers; Richard Read, *DEA Is Spying on Millions of U.S. Drivers with License Plate Readers*, WASH. POST (Jan. 27, 2015), http://www.washingtonpost.com/cars/dea-is-spying-on-millions-of-us-drivers-with-license-plate-readers/2015/01/27/96cb42c6-a644-11e4-a162-121d06ca77f1_story.html. The International Association of Chiefs of Police pointed out that automated license plate readers "may collect the license plate numbers of vehicles parked at locations that, even though public, might be considered sensitive, such as doctor's offices, clinics, churches, and addiction counseling meetings, among others." INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REP. FOR THE UTILIZATION OF LICENSE PLATE READERS 21 (2009).

44. *See* Jack Gillum, et al., *FBI Behind Mysterious Surveillance Aircraft Over U.S. Cities*, PBS (June 2, 2015), http://www.pbs.org/newshour/rundown/fbi-behind-mysterious-surveillance-aircraft-u-s-cities.

45. *See, e.g.*, William M. Bulkeley, *Chicago's Camera Network Is Everywhere*, WALL ST. J. (Nov. 17, 2009), https://www.wsj.com/articles/SB10001424052748704538404574539910412824756 (noting Chicago's police department links its 1500 cameras with thousands of other cameras deployed by other government agencies and the private sector); Mike Carter, *Judge Blocks Seattle from Revealing Locations of FBI's Hidden Cameras on Utility Poles*, SEATTLE TIMES (June 13, 2016), https://www.seattletimes.com/seattle-news/crime/judge-blocks-seattle-city-light-from-disclosing-locations-of-fbi-surveillance-cameras.

46. The tactical communications and surveillance catalog of British defense contractor Cobham was recently made public. It describes covert audio, video, and tracking surveillance equipment available to law enforcement agencies. *Product Quick Guide*, COBHAM TACTICAL COMMC'NS & SURVEILLANCE (Feb. 2014), https://www.cobham.com/media/1078613/Cobham_TCS_QuickGuide_Mar14.pdf.

worked with Microsoft to develop what it calls domain awareness system (DAS), which aggregates in real time various data from the city's public surveillance cameras, arrest records, lists of completed crimes and their characteristics, vehicle tracking information collected from license plate readers, and more.[47] Moreover, agencies, at all levels of government, that collect data frequently share it both within the agency and externally to other government entities,[48] though the terms of the use of that data often remain shrouded from public view.[49]

The government also acquires a great deal of information from the private sector. Some private-sector information comes from data-collection firms, such as ChoicePoint and Acxiom, that compile data from public records from around the country—information about births, marriages, divorces, property transactions, professional licenses, arrests, court proceedings, and more—and combine it with information from other sources, such as private detectives, as well as social media websites, property records, public health data, car rentals, utility bills, insurance claims, postal records, purchase history from discount and member-loyalty cards, and credit reporting firms, for sale to potential employers, landlords, and governments.[50] A

47. Joh, *supra* note 11, at 48–49; Press Release, Office of the Mayor, Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-of-the-Art Law Enforcement Technology That Aggregates and Analyzes Existing Public Safety Data in Real Time To Provide a Comprehensive View of Potential Threats and Criminal Activity (Aug. 8, 2012), http://www1.nyc.gov/office-of-the-mayor/news/291-12/mayor-bloomberg-police-commissioner-kelly-microsoft-new-state-of-the-art-law. As of 2013, the NYPD had a database of sixteen million license plates, along with the data regarding where they were captured. *Id.* Microsoft is also marketing this technology to other cities; New York City will receive thirty percent of the proceeds from future sales. *Id.*

48. *See, e.g.*, RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 19–47 (2013), https://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf.

49. *See, e.g.*, Larry Greenemeier, *What Is the Big Secret Surrounding Stingray Surveillance?*, SCI. AMERICAN (June 25, 2015), https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance.

50. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 142 (2013); Slobogin, *supra* note 16, at 320; Solove, *Digital Dossiers*, *supra* note 8, at 1151 (discussing government contracts with such private firms). This flow of information from the private sector grows ever larger as the government encourages the development of "new information-gathering technologies." *See Id.* at 1100. Information is big business. *See* Murphy, *supra* note 11 at 805–10 (2010) (discussing the history and current capacity of information databases); Solove, *Digital Dossiers*, *supra* note 8, at 1092

relatively new source of private-sector information is the Internet of Things—devices connected to the Internet that send and receive information—which allows the makers of products to track and record how they are used. Everything from thermostats to coffeemakers to baby monitors can be connected to the Internet, and information about those devices' use can be captured in databases,[51] the contents of which the government can then acquire.[52]

Together, the information the government collects through routine activity, intelligence operations, law enforcement tools, and deals with private-sector data brokers a bewildering amount of information with little, if any, particularized basis.[53] To be sure, some of this data collection is valuable—necessary even. Imagine trying to redraw congressional districts without the census, or collecting taxes without information about individuals' incomes. But this nonexhaustive list of the government's contemporary data-collection potential should convey the enormity of both its volume and its breadth.

("From credit reporting agencies, the government can glean information relating to financial transactions, debts, creditors, and checking accounts [as well as] details about people's race, income, opinions, political beliefs, health, lifestyle, and purchasing habits from database companies."); *id.* at 1084 ("In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities."). For evidence that information truly is big business, note that at one point ChoicePoint was valued at $3.6 billion. *Reed Elsevier To Acquire ChoicePoint for $3.6 Billion*, N.Y. TIMES (Feb. 21, 2008), https://www.nytimes.com/2008/02/21/technology/21iht-reed.4.10279549.html.

51. Bernard Marr, *Google's Nest: Big Data and the Internet of Things in the Connected Home*, FORBES (Aug. 5, 2015), https://www.forbes.com/sites/bernardmarr/2015/08/05/googles-nest-big-data-and-the-internet-of-things-in-the-connected-home/#6eb45273bac4.

52. *See* Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices for Spying*, GUARDIAN (Feb 9, 2016), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government. The same holds true for anything that conveys information about your movements and your purchases, such as items that contain a radio frequency identification (RFID) tag, which can include your passport, your credit card, your supermarket loyalty card, even the clothes that you wear. *See* Miguel Bustillo, *Wal-Mart Radio Tags To Track Clothing*, WALL ST. J., July 23, 2010, at A1; Alejandro Martınez-Cabrera, *Concern over Privacy As ID Tags' Use Expands*, S.F. CHRON., Sept. 6, 2010, at D1 (reporting that a California county implanted RFID tags in preschoolers' uniforms).

53. *See* Joh, *supra* note 11, at 39 (noting that ninety percent of the world's data has been generated in the past two years, and that we now create as much information in two days as we did from the beginning of human civilization until 2003).

B. THE AGGREGATION PROBLEM

Though the volume and variety of information to which the government has access raises its own questions, my primary concern is what the combination (aggregation) of so much information enables the government to discover. Analysis can derive from data that private information, "at the time of their collection, seemed to raise no, or only manageable, privacy issues."[54] Professor Solove has called this phenomenon the aggregation problem.[55] When seen "in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about" us.[56] The upshot is

54. PRES.'S COUNCIL OF ADVISORS ON SCI. & TECH., BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE at ix (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [hereinafter PCAST].

55. Solove, *Access and Aggregation*, *supra* note 36, at 1185; *see also* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008) (noting that technologies allow the government "to record perfectly innocent behavior that no one is particularly ashamed of and draw from that data surprisingly powerful inferences about people's behavior, beliefs, and attitudes"); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework To Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93, 106 (2014) ("[O]ne cannot assess the predictive privacy risks from the collection of a single data point."); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 826 (2015) (discussing how a fusion of locational-body surveillance and biographical-behavioral surveillance allows the government to enable tracking and data analytics on potential suspects and/or terrorists); Solove, *Digital Dossiers*, *supra* note 8, at 1154 ("A fact here or there may seem innocuous but when combined, they become more telling about that person.").

The aggregation problem is related to, but is distinct from, what has been labeled mosaic theory, which posits that "a series of acts that are not searches in isolation amount to a search when considered as a group." *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012). The idea is that multiple nonsearches combined together may amount to a search because of the mosaic they reveal. *Id.* The quintessential example is the long-term surveillance of an individual's public movements—combining a sufficient number of location data points over a sufficient period of time will reveal a great deal of information about the surveillance target's life. While the mosaic theory describes one form of aggregation—the aggregation of information resulting from a series of government collection activities—it is focused on determining when a sequence of government acts constitutes a search. By contrast, I do not argue that a series of nonsearches becomes a search when a certain threshold is crossed. Instead, I argue that the single act of querying a database can itself be a search. *See infra* notes 221–24 and accompanying text.

56. Solove, *Access and Aggregation*, *supra* note 36, at 1185; *see also* PCAST, *supra* note 54, at x (noting that aggregating data "can result in the identification of individual people, the creation of profiles of an individual, and the tracking of an individual's activities").

that when government officials search—or query—aggregated information, they can learn a great deal more about the subject of the query than they could have done using any individual piece of data alone. Importantly, the additional information data aggregation provides may be "precisely the same information [the government] previously would have been required to obtain a warrant to access," thereby undermining existing privacy protections.[57]

Think of the aggregation problem as the difference between explicit and implicit knowledge.[58] Explicit knowledge is information that is plain on the face of data. Implicit knowledge is information that can be extracted through data analysis.[59] Consider the following hypothetical. Jane's neighbor (or the license plate reader in her neighborhood) knows that, beginning two months ago, she started leaving for work one hour earlier on Thursday mornings than on other workdays; the grocery store clerk (or the grocery store's member-loyalty program) knows that over that same time frame, Jane has eaten a pint of coffee ice cream every week; and the barista at a coffee shop on the other side of town (or the coffee shop's frequent-customer program) knows that she recently became a Thursday morning regular.

Standing alone, each of these disclosures reveals only a small amount of information about Jane, none of which is particularly sensitive. But imagine that each of these facts was digitally stored in a government database, which investigators

57. TECH. & PRIVACY ADVISORY COMM., U.S. DEP'T OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 36 (2004), https://www.cdt.org/files/security/usapatriot/20040300tapac.pdf.

58. K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots To Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 3, 37 (2003).

> Extracting *implicit* information means that the results of data mining are not existing data items in the database. Traditional information retrieval from a database returns arrays consisting of data from individual fields of records (or entire records) from the database in response to a defined or specified database query. The results of the traditional database query are explicit in the database, that is, the answer returned to a query is itself a data item (or an array of many items) in the database. Data mining techniques, however, extract knowledge from the database that is implicit—knowledge that typically does not exist a priori is revealed.

Id. (internal citations and quotations omitted).

59. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (noting that momentary location information is not particularly revealing, but aggregating location information can generate "a precise, comprehensive record" of a person's life, reflecting "a wealth of detail about her familial, political, professional, religious, and sexual associations").

can then query for all of the information it contains about Jane. The results of that query could easily lead to the conclusion (whether correct or incorrect) that something in Jane's life changed two months ago and that she now has a weekly Thursday morning appointment somewhere near a particular coffee shop. Further investigation into this Thursday morning activity could reveal regular trips to a psychiatrist, a fertility clinic, a substance abuse rehabilitation center, or any number of other intensely personal activities that neither a neighbor nor a barista could divine with the isolated bits of information available to them. In other words, querying a database compiled from disparate sources "reveals facts about data subjects in ways far beyond anything they expected" based on what they have revealed publicly.[60] The whole is more than the sum of its parts.

The threat posed by aggregation is not limited to hypotheticals. The NSA's post-9/11 surveillance programs illustrate the aggregation problem's implications. The now-discontinued Section 215 bulk telephone metadata surveillance program (named after the relevant statutory provision of the USA PATRIOT Act)[61] involved collecting and aggregating all of Americans' telephony metadata, thereby compiling an enormous volume of Americans' telephone communications records.[62] Government analysts could then query that database using a seed identifier, basically a search term (here, usually a phone number), to extract information regarding a particular individual.[63] A query yields "phone numbers, and the metadata associated with

60. Solove, *A Taxonomy of Privacy*, *supra* note 10, at 508; Solove, *Access and Aggregation*, *supra* note 36, at 1178 ("We know that our lives will remain private not in the sense that the information will be completely shielded from public access, but . . . because it is a needle in a haystack, and usually nobody will take the time to try to find it.").

61. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 277–78 (2001) (codified as amended at 50 U.S.C. § 1861 (2012)) (permitting the FBI to "make an application for an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information . . . or to protect against international terrorism or clandestine intelligence activities"). The USA FREEDOM Act of 2015 eliminated the use of Section 215 for bulk collection. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861).

62. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 8 (2014), https://www.pclob.gov/library/215-report_on_the_telephone_records_program.pdf [hereinafter PCLOB SECTION 215 REPORT].

63. *Id.* at 26–31.

them, that have been in contact with the seed."[64] At that point, the government can then search for the numbers and associated metadata that have been in contact with the numbers the first query returns.[65] So rather than simply getting the list of numbers with which the seed is in contact, the aggregation of all metadata allows the government to map the entire communications network of the seed number.[66] Even conceding for the sake of argument that the collection of a single, targeted individual's phone records does not raise privacy concerns,[67] the capabilities exercised in the Section 215 metadata program might give us pause. Indeed, it gave the American public pause when it came to light.[68]

Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act provides an even more troubling illustration, as that program authorizes the government to collect communications content,[69] which the Constitution has always treated as one of the most intrusive forms of surveillance.[70] The program collects the electronic communications into and out of the United States of a target "reasonably believed to be located outside the United States."[71] Electronic communications in-

64. ACLU v. Clapper, 785 F.3d 787, 797 (2d Cir. 2015).

65. *Id.*; PCLOB SECTION 215 REPORT, *supra* note 62, at 29 ("[Investigators are] able to view the records of calls involving telephone numbers that had contact with a telephone number that had contact with the original target.").

66. Identifying unknown targets through scrutiny of an individual's social networks is known as link analysis. Statement of Nathan A. Sales, Asst. Prof., George Mason Sch. of Law, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., WORKSHOP REGARDING SURVEILLANCE PROGRAMS OPERATED PURSUANT TO SECTION 215 OF THE USA PATRIOT ACT & SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 2 (July 9, 2013).

67. This is the current state of the law according to the third-party doctrine. *See infra* notes 81–92 and accompanying text (discussing the third-party doctrine).

68. After the Section 215 program became public in 2013, President Obama slightly curtailed its scope; the USA FREEDOM ACT of 2015 then enacted several modifications, including a bar on bulk collection. *See* Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES (June 2, 2015), https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html.

69. 50 U.S.C. § 1881a (2012). Contrast this to the Section 215 program, which collected only metadata, which traditionally enjoys much less constitutional protection than content.

70. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741 (1979) (distinguishing a prior case which acquired the contents of a phone conversation from acquiring the number dialed).

71. 50 U.S.C. § 1881a(g)(2). Upon discovery that "a Section 702 target is a U.S. person or was inside the United States at the time of targeting, the gov-

cludes the contents of phone calls and email, as well as instant messages, Facebook messages, web browsing history, and Skype conversations.[72] And while the government may neither target a U.S. person nor target a foreigner for the purpose of acquiring a particular U.S. person's communications, communications collected under this program necessarily include someone in the U.S.[73] This results, of course, in the collection of "a significant amount of information about U.S. persons."[74] Analysts may then query the database of Section 702–acquired information using a seed associated with a U.S. person, thus accessing any conversation that a particular U.S. person had with an overseas target.

The aggregation problem arises outside the foreign intelligence context as well. As Justice Sonia Sotomayor eloquently made plain in her concurrence in *United States v. Jones*, aggregating information about an individual's location over a substantial period of time generates "a wealth of detail about her familial, political, professional, religious, and sexual associations."[75] Investigators can extract location information by aggregating sufficiently extensive networks of cell tower simula-

ernment must stop the collection immediately," but is permitted to "waive" the general requirement that such communications must be destroyed. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 127 (2014), https://www.pclob.gov/library/702-report.pdf [hereinafter PCLOB SECTION 702 REPORT].

72. *See, e.g.*, Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 120 (2015).

73. PCLOB SECTION 702 REPORT, *supra* note 71, at 127–33.

74. *Id.* at 133; *see also* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

75. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Similar information could be acquired by collecting CSLI in bulk. For a discussion of CSLI, see *supra* note 40. To date, no government agency has tried to acquire a comprehensive database of all CSLI (as far as I am aware), but a sufficient number of cell tower simulators deployed across a particular geographical area, would provide the same data. A query of a widely distributed network of automatic license plate readers (ALPR) fed into a single database regarding a particular individual's vehicle—a criminal suspect, an ex-girlfriend—would also return a map of that individual's movements. In a 2011 survey by the Police Executive Research Forum, seventy-one percent of responding agencies used ALPRs and eighty-five percent planned to acquire or increase their use over the next five years. POLICE EXEC. RESEARCH FORUM, HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING? 31 (2012), http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.

tors, surveillance cameras, automatic license plate reader (ALPR) technology, biometric information, or databases with records from companies such as E-Z pass, Travelocity, or Hotels.com.[76]

You might wonder why we should be concerned about the information that the government collects and the kind of conclusions it can draw from aggregating and searching that information. After all, doesn't the Fourth Amendment protect our privacy? Wouldn't the Constitution bar the government's access to truly private information absent probable cause to believe criminal activity is afoot? As the next Part will make plain, the answer to both of these questions is an emphatic no.

II. FOURTH AMENDMENT LAW'S FAILURE

To fall within the Fourth Amendment's ambit, government action must qualify as a search or seizure. The current regime defining searches for Fourth Amendment purposes began in 1967, with *Katz v. United States*.[77] In *Katz*, the Supreme Court rejected the idea that the Fourth Amendment regulates only physical trespasses by government officials, holding that it protects "people, not places."[78] As a result, collecting the contents of a phone call made from a public telephone booth qualified as a search requiring a warrant.[79] Since *Katz*, the Fourth Amendment has regulated any government activity that violates an individual's reasonable expectation of privacy.[80]

Such activity constitutes a search and must comply with constitutional limits. Usually those limits require the government to secure a warrant from a neutral magistrate based upon probable cause.

As Section A demonstrates, however, under contemporary doctrine, a great deal of information collection does not violate a reasonable expectation of privacy; even when it does, an exception to the warrant requirement often applies. Moreover,

76. The FBI's database of biometric information includes millions of photographs. U.S. GOV'T ACCOUNTABILITY OFFICE, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 10 (2016), https://www.gao.gov/assets/680/677098.pdf. This database is used by both federal and state investigators. *Id.* at 11.

77. 389 U.S. 347 (1967). Prior to *Katz*, the Fourth Amendment regulated government activity that physically invaded protected spaces, like houses or offices. *Id.* at 352–53.

78. *Id.* at 351.

79. *Id.* at 353.

80. *Id.* at 361 (Harlan, J., concurring).

the absence of constitutional limits regarding the government's use of that information, as Section B will explain, magnifies any concerns raised by the dearth of Fourth Amendment limits on collection. Section C will then demonstrate how recent Supreme Court cases reveal the tension that the power of information aggregation is currently creating within Fourth Amendment doctrine.

A. THE FOURTH AMENDMENT'S PERMISSIVE INFORMATION COLLECTION RULES

This Section discusses two circumstances in which the warrant requirement does not apply. First, what I call Fourth Amendment *exemptions* refer to instances in which the collection at issue does not qualify as a search or seizure. The Supreme Court's interpretation of *Katz*'s reasonable-expectation-of-privacy test places an enormous amount of information—some of it highly sensitive—in this category. Second, I refer to instances where the Fourth Amendment applies but the government need not secure a warrant as warrant requirement *exceptions*. In those circumstances, the government action must merely be reasonable, a determination courts make by balancing the government's interest in collection against the intrusiveness of the search or seizure. This Section will show how these exemptions and exceptions often swallow the Fourth Amendment rule.

Three preliminary points are in order. First, this Section does not provide an exhaustive catalog of Fourth Amendment exceptions and exemptions. It should, however, illustrate the permissiveness of the overall regime. Second, in this Article I take no position in the heated, long-running debate regarding the appropriate scope of existing exemptions and exceptions. Instead, I simply expound existing doctrine. Third, I recognize that the collection of information that enjoys no Fourth Amendment protection may nevertheless be subject to statutory or regulatory limits. As I explain in Part III, *infra*, I find those types of limits unsatisfactory as a general matter; moreover, even with the most stringent collection rules, the aggregation problem would still present a privacy threat.

1. Fourth Amendment Exemptions

Of the numerous Fourth Amendment exemptions, those responsible for most of the investigative activity relevant to the aggregation problem come from one of two doctrines. First is

the third-party doctrine, by far the most significant Fourth Amendment exemption.[81] The doctrine provides that any information we voluntarily reveal to a third party—a term encompassing any individual or nongovernmental institution—enjoys no Fourth Amendment protection.[82] In *Smith v. Maryland*, one of the doctrine's foundational cases, the Supreme Court held that law enforcement's collection of the list of phone numbers that a criminal suspect dialed did not constitute a search because the suspect should have reasonably expected that his telecommunications provider kept track of such information and he had therefore voluntarily relinquished it.[83] By relinquishing this information to another, the doctrine reasons, one cedes any reasonable expectation of privacy in it.[84]

Consider what is included in this category of information: phone records identifying who you associate with; bank records showing who you do business with; credit card records revealing where you eat, shop, and seek entertainment; medical records listing your prescriptions; the records of cable companies and video-streaming services exposing what you watch; Internet browsing history indicating whether you have searched for symptoms of disease or investigated substance abuse treatment options; and travel records from airlines, hotels, rental car companies, or other third parties like Orbitz or Kayak.[85] The third-party doctrine also denies Fourth Amendment protections to information that private firms gather from your appliances.[86]

81. The third-party doctrine has never been well loved by commentators, and members of the academy continue to produce suggestions to eliminate or modify it. *See, e.g.*, Kerr, *supra* note 8, at 563–64 nn.5–11 (compiling a list of critiques of third-party doctrine); Peter P. Swire, *Katz Is Dead. Long Live Katz.*, 102 MICH. L. REV. 904 (2004); *see also* sources cited *supra* note 8.

82. *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

83. *Maryland*, 442 U.S. at 743–45.

84. *Id.*

85. *See* Solove, *Digital Dossiers*, *supra* note 8, at 1090–91.

86. *Id.* A particularly aggressive interpretation of the third-party doctrine was also used to justify the NSA's warrantless bulk collection of telephone metadata. Under that program, rather than simply collecting the call records of a particular individual, as it had done in *Smith*, the government collected all of the telephony metadata recorded by communications providers of all calls made through their system where one or both ends of the communication were in the United States. ACLU v. Clapper, 785 F.3d 787, 795–99 (2d Cir. 2015); *see also supra* notes 70–85 and accompanying text, *infra* notes 87–110 and accompanying text. And, because both the government and the FISC agreed that telephone metadata qualified as third-party records that are not

To be sure, some of the data subject to collection under the third-party doctrine is subject to statutory or policy-based rules. To collect an individual's communications metadata under Section 215, for example, the government must certify that the "information likely to be obtained" is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[87] And the Attorney General must "include privacy protections that apply to the collection, retention, and use of information concerning United States persons."[88] Medical records also enjoy statutory protection.[89] But as privacy scholars have demonstrated repeatedly, the existing legal framework for protecting individual privacy is, on the whole, outdated and incomplete.[90]

Note that the principle behind the third-party doctrine—the idea that anything you have voluntarily provided to a third party lacks Fourth Amendment protection—is not limited to written records. The third-party doctrine's close cousin, sometimes referred to as the "false friend" doctrine, applies the same idea to spoken conversations.[91] There is no reasonable expectation of privacy in what someone voluntarily tells an interlocutor, even if—unbeknownst to the speaker—she happens to be a government agent or informant.[92] This doctrine allows law enforcement or intelligence officials to attend and record (or task informants to attend and record) religious or political gather-

entitled to Fourth Amendment protection, the government was able to assemble a vast database made up of an enormous volume of Americans' telephone communications records, both domestic and international, with no constitutionally imposed limits. Amended Memorandum Opinion at 3, *In re* Application of FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109 (FISA Ct., Aug. 29, 2013).

87. 50 U.S.C. § 1842(c)(2) (2012). Metadata collected in the criminal context must be "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2) (2012).

88. 50 U.S.C. § 1842(h)(1).

89. Slobogin, *supra* note 24, at 158.

90. *See, e.g.*, Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233 (2004) (noting that one particular privacy statute is "vague in some places, overly complex in others, and underprotective of privacy interests in others"); Slobogin, *supra* note 24, at 149–67 (describing limited privacy protections for information other than communications content); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 364–68 (2006) (describing the "limits of U.S. privacy law"); *see* sources cited *infra* notes 251–52.

91. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1326 (2012).

92. *E.g.*, Hoffa v. United States, 385 U.S. 293, 296 (1966).

ings as well as individual conversations.

While the third-party doctrine is the most noteworthy Fourth Amendment exemption, another is also quite significant. The Supreme Court held in *Knotts v. United States* that when government officials collect information about one's physical location in a public place—even if aided by an electronic tracking device—that collection is neither a search nor a seizure.[93] The Court reasoned that people "traveling in an automobile on public thoroughfares" voluntarily convey the details of their travels "to anyone who want[s] to look."[94] Under a broad reading of *Knotts*, the government could argue that the Fourth Amendment does not apply to any location-tracking method so long as the government has not trespassed on private property to collect the information.[95] Cell site location information (CSLI) gathered through the use of a cell tower simulator or from a communications provider,[96] video surveillance paired with facial-recognition software, toll records, or license plate readers all can be viewed simply as a means of collecting location information. So long as the resulting data is limited to locations in public places, *Knotts* arguably permits such acquisition as merely the gathering of information voluntarily divulged to the public at large. Regulations addressing these forms of collection, if they exist, vary from jurisdiction to jurisdiction.[97]

2. Warrant Requirement Exceptions

In circumstances where the Fourth Amendment applies but the warrant requirement does not, the traditional limits of ex ante review, probable cause, and particularity become fall away. In these cases, the Fourth Amendment merely requires that, taking into account the totality of the circumstances, the government search or seizure is "reasonable." Courts determine

93. United States v. Knotts, 460 U.S. 276, 282 (1983); *see also* United States v. Karo, 468 U.S. 705 (1984) (holding that the use of a beeper to track a person's location was not a search under the Fourth Amendment until the beeper entered a home).

94. *Knotts*, 460 U.S. at 281–82; *cf. Karo*, 468 U.S. at 731–32 (holding that the Fourth Amendment is only violated by the warrantless location search of a container at the moment it enters a private home).

95. *See* United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring).

96. For information on CSLI's constitutional status, see discussion *supra* note 40.

97. Solove & Hoofnagle, *supra* note 90, at 380–82.

whether government action is reasonable by balancing the government's interest against the intrusiveness of the search; reasonableness sometimes, but not always, requires individualized suspicion.[98]

The most important warrant requirement exception for the purposes of this Article is the foreign-intelligence-surveillance exception.[99] Under this exception, the government need not secure a warrant to collect information with foreign intelligence value.[100] In *In re Directives*, the Foreign Intelligence Surveillance Court of Review (FISCR)[101] held that, "a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against [targets] reasonably believed to be located outside the United States."[102] The FISCR also found the surveillance pro-

98. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 30 (1968) (holding stop-and-frisk searches permissible with reasonable suspicion that the person is "armed and presently dangerous"); Warden v. Hayden, 387 U.S. 294, 298–300 (1967) (creating an "exigent circumstances exception" to the warrant requirement for home searches); Carroll v. United States, 267 U.S. 132, 153 (1925) (allowing for warrantless search of vehicles with reasonable suspicion of crime); *see also* California v. Carney, 471 U.S. 386, 393–95 (1985) (extending vehicle exception to mobile homes in certain circumstances).

99. The foreign intelligence surveillance exception is actually just one application of a broader warrant requirement exception known as the special needs doctrine. That doctrine provides that a warrantless search may be justified when special needs, "beyond the normal need for law enforcement," make the warrant and probable-cause requirements of the Fourth Amendment impracticable. *E.g.*, New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). Under this rationale, the Supreme Court has approved as consistent with the Fourth Amendment: (1) the U.S. Customs' Service's mandatory drug testing of employees seeking promotion to positions involving interdiction of illegal drugs, requiring them to carry firearms, or requiring them to handle classified materials; (2) a school district's random drug testing for student athletes; (3) the search of a probationer's home; and (4) numerous other contexts. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665–66 (1989); Griffin v. Wisconsin, 483 U.S. 868, 873, 875 (1987). *See also* Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822 (2002) (holding that individualized suspicion is not required to justify random drug testing of students involved in extracurricular activities); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602 (1989) (holding that warrantless drug and alcohol tests for railway employees were reasonable even in the absence of reasonable suspicion that any particular employee was impaired).

100. *T.L.O.*, 469 U.S. at 336.

101. FISA created a Court of Review (FISCR), made up of three federal district or appeals court judges appointed by the Chief Justice, to hear appeals from decisions of the FISC. 50 U.S.C § 1803 (2012).

102. *In re* Directives, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). *In re Direc-*

gram as a whole reasonable and therefore lawful under the Fourth Amendment.[103]

This case gave a green light to the Section 702 program's collection of non-U.S. persons' electronic communications, so long as the target is "reasonably believed to be located outside the United States."[104] If the government directly targeted U.S. persons for their international electronic communications, such surveillance would indisputably require individualized probable cause.[105] Yet because the program both qualifies for the foreign-intelligence-surveillance exception to the warrant requirement and has been deemed reasonable by the FISCR, the Fourth Amendment poses no obstacle to this collection—even in the absence of individualized suspicion about the overseas target's American interlocutors.[106]

As with communications metadata, Section 702 collection and the use of the resulting data are subject to some statutory, policy-based, and judicially imposed limits.[107] For example, a "significant purpose" of the collection must be to gather foreign intelligence information—a relatively expansive category[108]—

tives involved a challenge to the temporary Protect America Act (PAA), Pub. L. No. 110-55, § 105B, 121 Stat. 552 (2007). The PAA was replaced in 2008 by the FISA Amendments Act (FAA), Pub. L. No. 110-261 (codified at 50 U.S.C. §§ 1881a–g).

103. *In re Directives*, 551 F.3d at 1012–15. The FISCR held that the surveillance met the Fourth Amendment's reasonableness requirement in light of the government's interest in protecting national security and the "matrix of safeguards" that mitigated the intrusiveness of the program. *Id.*

104. *Id. See* 50 U.S.C. § 1881a(g)(2).

105. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972); 50 U.S.C. §§ 1801–1805.

106. *In re Directives* implied that an executive order requiring the Attorney General to have probable cause to believe that the targeted person is a foreign power or its agent was one of several constitutionally compelled procedural protections. *In re Directives*, 551 F.3d at 1014.

107. *See, e.g.*, 50 U.S.C. §§ 1861, 1881a; ERIC H. HOLDER, JR., ATT'Y GEN. OF U.S., PROCEDURES USED BY THE NSA FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES (2009) (detailing NSA targeting procedures); Berman, *supra* note 33, at 806–17 (detailing the judicially imposed limits on Section 215 and Section 702 data); Peter Margulies, *Reauthorizing the FISA Amendments Act: A Blueprint for Enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities*, 12 J. BUS. & TECH. L. 23, 37–39 (2016) (describing judicially and executive-branch-imposed limits on data collection).

108. *See* 50 U.S.C. § 1801(e). A target of Section 702 surveillance "could be completely innocent." *Hearing on Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties Before the S. Comm. on the Judiciary*, 114th Cong. 7 (2016) (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight

but it need not be the only purpose.[109] Indeed the primary purpose of the collection could be something totally unrelated—such as a criminal investigation.[110] And while queries of the Section 702–acquired information are themselves subject to rules developed in conjunction with the FISA,[111] those rules do not prevent the most troubling practice (from a Fourth Amendment perspective, anyway): analysts may perform so-called U.S. person queries, which ask for communications involving a particular U.S. person. Such a query returns all international communications that U.S. person engaged in with any overseas target, regardless of its foreign intelligence value.[112] This occurs despite the statute barring the targeting of U.S. persons for collection.[113]

Other courts have relied on the foreign-intelligence-surveillance exception to bless the warrantless search of a U.S. citizen's home in Kenya[114] as well as New York City's suspicionless searches of individuals riding the subway.[115] The list of warrant requirement exceptions is long—it includes searches or seizures of items in plain view, border searches,[116] inventory searches, consent searches, and more.[117]

Board). For an argument that a broad definition of "foreign intelligence information" is necessary to successful diplomacy, see Peter Margulies, *Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 WASH. & LEE L. REV. 1283, 1283–87 (2015).

109. 50 U.S.C. § 1881a(g)(2)(A)(v).

110. The NSA determines who will be targeted, but the FBI may "nominate" targets. PCLOB SECTION 702 REPORT, *supra* note 71, at 47.

111. *See* NAT'L SEC. AGENCY, U.S. SIGNALS INTELLIGENCE DIRECTIVE, USSID SP0018, LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES § 4 (2011); NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT § 3 (2007); William C. Banks, *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, 51 U. RICH. L. REV. 671, 672–88 (2017) (detailing nonconstitutional limits on Section 702 data collection and use).

112. In 2016, the government (not including the FBI, which is exempt from reporting requirements) used 5288 search terms associated with a U.S. person. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES FOR CALENDAR YEAR 2016, at 8 (2017).

113. *In re* Directives, 551 F.3d 1004, 1012–15 (FISA Ct. Rev. 2008).

114. *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93 (2d Cir. 2008).

115. MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006) (permitting application of the special needs exception to a warrantless search where the subject of a search possesses a full privacy expectation).

116. *See* United States v. Ramsey, 431 U.S. 606, 616 (1977) (finding that

This brief discussion of a couple of those exceptions, however, shows that the default Fourth Amendment rule requiring a showing of probable cause, identification of the object of the search or seizure with particularity, and ex ante approval by a neutral magistrate does not always apply. In fact, there are many circumstances in which the government constitutionally may collect large swaths of information about Americans without satisfying one or more of the traditional Fourth Amendment limits, and often without any individualized suspicion at all.

B. THE FOURTH AMENDMENT'S (NON)EXISTING USE-RESTRICTION RULES

The government's broad collection rules plainly raise their own privacy concerns, but even if they did not, postcollection use would still pose such threats. Indeed, the government's broad collection power might not be so alarming if there were reliable limits on how the government used the information in its possession. As this Section will demonstrate, however, the conventional wisdom is that once data is in the government's hands, the Constitution has nothing to say at all.[118] In the

routine searches of people and their effects at the border are "reasonable simply by virtue of the fact that they occur at the border"). The advent of digital storage devices, such as laptops, cell phones, and thumb drives, has generated numerous questions regarding the application of the border search doctrine to the contents of these devices. The Supreme Court has not yet weighed in on the issue, but courts addressing the question have consistently held that routine inspection of electronic media—which would include booting up a device, reviewing its contents, and using search functions to find and review specific files—is permissible, even in the absence of suspicion. *See, e.g.*, United States v. Saboonchi, 990 F. Supp. 2d 536, 549 (D. Md. 2014); United States v. Ickes, 393 F.3d 501, 502–03 (4th Cir. 2005). The rule is slightly less permissive when it comes to forensic border searches, which generally entail making a mirror of the entire contents of the digital device, and then subjecting that copy to scrutiny using analytic software to recover hidden, deleted, or encrypted data. *See* Saboonchi, 990 F. Supp. 2d at 547–48. To engage in forensic searches, the government must have individualized suspicion, which is not a particularly high bar. *Id.* at 570 ("This standard is far from onerous.").

117. *See Investigations and Police Practices—Warrantless Searches and Seizures*, 44 GEO. L.J. ANN. REV. CRIM. PROC. 48 (2015) (listing additional exceptions to the warrant requirement).

118. *E.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1173 (9th Cir. 2010) ("It goes without saying that lawfully seized evidence may not be suppressed."); Boroian v. Mueller, 616 F.3d 60, 67–68 (1st Cir. 2010) (retaining a former offender's DNA profile "does not constitute a separate search under the Fourth Amendment"); *see also* Balkin, *supra* note 55, at 20 ("[B]ecause the Fourth Amendment focuses on searches and seizures, it places few limits on collation and analysis."); Joh, *supra* note 11, at 63 ("If

words of one respected jurist, "the [F]ourth [A]mendment does not control how properly collected information is deployed."[119]

Whatever logic this constitutional vacuum may have had in the past, the absence of use restrictions cannot persist in the face of the convergence of two factors. First, there remains very little information about what we do, where we go, what we purchase, or with whom we communicate that some third party does not record and store digitally. This means the government will have access to an ever-growing amount of information about each individual American. Similarly, we now live in a networked world. Many Americans have family, friends, or business associates all around the globe. With international communications ubiquitous and—so long as you can find a Wi-Fi connection—free, long distance phone charges are a thing of the past. Moreover, much of this international interaction takes place through modes of communication—e-mails, instant messages, video and voice chats, videos, photos, voice-over-IP (such as Skype or FaceTime), and other digital tools—that are subject to collection under the Section 702 program.[120] Accordingly, a great deal more of our communications are likely vulnerable to collection.

Second, contemporary technology permits the government to collect, store, aggregate, and analyze large volumes of data in ways that were either unavailable or cost prohibitive for most of America's history.[121] So even as we generate more and more digital information about ourselves, the government's ca-

[information] acquisition is permissible, how the police use that information thereafter is generally not subject to an additional Fourth Amendment challenge."); Kerr, *supra* note 22, at 6 ("If the government comes across information legally, then it is free to use that information however officials would like."); Erin Murphy, *Back to the Future: The Curious Case of* United States v. Jones, 10 OHIO ST. J. CRIM. L. 325, 330–31 (2012) ("Current Fourth Amendment law emphasizes acquisition . . . . It cares little for what happens next—to what use that information is put."); William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 857 (2001) ("Fourth Amendment law regulates the government's efforts to uncover information, but it says *nothing* about what the government may do with the information it uncovers.").

119. Green v. Berge, 354 F.3d 675, 680 (7th Cir. 2004) (Easterbrook, J., concurring).

120. Greenwald & MacAskill, *supra* note 74; *see also supra* notes 70–110 and accompanying text (describing the Section 702 program).

121. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (discussing the impact of changing technologies on Fourth Amendment doctrine).

pacity for exploiting that information grows.[122] Thanks to contemporary technology, government information collection and analysis powers have grown substantially in recent decades. And while over time there have been some technology-driven changes to constitutional rules regarding government collection, the rules (or lack of them) when it comes to information use have remained stagnant.

C. THE FOURTH AMENDMENT IN THE DIGITAL AGE

Two recent Supreme Court cases starkly illustrate the pressure that modern technology places on existing Fourth Amendment doctrine. In *United States v. Jones* and *Riley v. California*, the Supreme Court recognized the transformative nature of data aggregation and considered whether current doctrine needs to be modified in response.[123] *United States v. Jones* presented almost exactly the same question that *Knotts* considered nearly three decades earlier—whether tracking a vehicle's location on public thoroughfares over time constitutes a search[124]—a question that *Knotts* answered in the negative.[125] *Jones* presented the issue, however, in a more technologically sophisticated context: whether law enforcement had engaged in an unlawful search when it placed a GPS device on a suspect's car without a valid warrant and used it to collect a detailed account of his movements over the course of several weeks.

122. Solove, *A Taxonomy of Privacy*, *supra* note 10, at 497 (comparing an automobile tracking device to the historic practice of police following a defendant on a highway or street).

123. The need for Fourth Amendment doctrine to accommodate technological change did not suddenly arise for the first time in the twenty-first century. Doctrine began grappling with technology's effects by at least the 1920s. In *United States v. Lee*, 274 U.S. 559, 563 (1927), for example, the Supreme Court held that the Coast Guard did not engage in a search when it used a searchlight to illuminate otherwise hidden cases of alcohol on a boat during the Prohibition Era. *See also* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imaging device to monitor the radiation of heat from a home is a search). Throughout American history, as investigative methods have evolved, courts have continuously recalibrated the doctrine, sometimes announcing new rules, sometimes simply explaining how the old rules applied to new contexts. *See*, *e.g.*, Katz v. United States, 389 U.S. 347, 352–53 (1967); *see also* Kerr, *supra* note 27, at 531 (explaining how courts adjust Fourth Amendment doctrine in response to technology to maintain the balance of power between would-be criminals and the government).

124. United States v. Jones, 565 U.S. 400, 402 (2012).

125. United States v. Knotts, 460 U.S. 276, 282 (1983); *see also supra* notes 93–95 and accompanying text.

While the *Jones* majority opinion rested its holding that this *did* constitute a search on the decidedly nontechnological fact that government officials "physically occupied private property" when they placed the GPS device on Jones's car,[126] two concurrences (representing five justices) recognized that the case implicated larger questions about how the Fourth Amendment should approach technological advances. Justice Alito argued that long-term GPS surveillance violates a reasonable expectation of privacy.[127] Justice Sotomayor explained how several technological factors have combined to change the nature—and hence the intrusiveness—of location information since the Court decided *Knotts*.[128] Contemporary monitoring tools provide a much more detailed, complete set of data,[129] and are much more likely to be used because they are cheap and invisible.[130] Justice Alito made a similar point when observing that, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[131] Moreover, Sotomayor pointed out, once collected, the government can "store such records and efficiently mine them for information years into the future."[132] As a result, Justice Sotomayor concluded, such collection is fundamentally *different in kind* from physical surveillance aided by a beeper like the one in

126. *See Jones*, 565 U.S. at 404.

127. *Id.* at 430–31 (Alito, J., concurring).

128. *Id.* at 414 (Sotomayor, J., concurring).

129. *Id.* at 414–16 (noting the extensive personal information that use of GPS devices can generate, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on").

130. *Id.* at 416 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)) (noting the low cost and minimal manpower required for GPS surveillance allow the government to evade "the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'"); *see also Jones*, 565 U.S. at 429–30 (Alito, J., concurring) (arguing that historically the most effective privacy protections were practical rather than constitutional or statutory and that the monitoring at issue in *Jones* "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," a use of resources that would only have been limited to "investigation[s] of unusual importance"); Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 341–50 (2014).

131. *Jones*, 565 U.S. at 429 (Alito, J., concurring).

132. *Id.* at 415 (Sotomayor, J., concurring).

Knotts.[133] Courts must "take these attributes," she argues, "into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."[134]

To be sure, the government might obtain the exact same information through analog surveillance techniques as it could via long-term GPS monitoring.[135] But this does not mean that GPS monitoring poses the same level of intrusion as conventional surveillance. For most of our history, practical impediments precluded law enforcement from collecting the information captured by GPS devices. Law enforcement is unlikely to invest the resources required to follow someone like Jones, who was suspected of possession with the intent to distribute cocaine, twenty-four hours a day for several weeks. Moreover, due to these practical constraints, courts never had to face the question whether months-long twenty-four-hour surveillance constituted a search. Hence Justice Sotomayor's conclusion that the surveillance at issue in *Jones* presented a novel question not controlled by short-term surveillance cases like *Knotts*. In eliminating these practical obstacles to physical surveillance, technological advances do not only permit more collection. More importantly, the volume of collection amounts to an entirely new sort of surveillance: the results of aggregating that data, enabling the government to extract knowledge (intimate details abut our daily lives, activities, and relationships) in which we have always had a reasonable expectation of privacy. Now that technology has eliminated the practical obstacle to aggregating large amounts of location information, the courts must erect a doctrinal bulwark to protect that expectation of privacy.

In other words, certain technology, when combined with storage and analysis capacity, raises the aggregation problem in a way that implicates reasonable expectations of privacy. At least five members of the Court recognized the distinction between government access to information revealed piecemeal (an individual's location in public at any given moment in time) and access to an extensive dossier assembled by aggregating many isolated pieces of information (the compilation of weeks of information about Jones's vehicle's location).[136] The D.C. Cir-

133. *Id.*

134. *Id.* at 416.

135. *Id.* at 415.

136. *See id.* at 413, 418 (Sotomayor, J., concurring and Alito, J., concurring).

cuit Court's Judge Ginsburg perhaps put it best when he explained in the lower court's opinion in *Jones* that,

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[137]

So while we may have no reasonable expectation of privacy in one piece of information about our location in public, the calculus regarding long-term GPS surveillance is different, given the conclusions one can draw from the aggregation of location information spanning several weeks.

In *Riley v. California*, the Supreme Court also acknowledged the potential intrusiveness facilitated by modern technology's ability to aggregate large amounts of information.[138] *Riley* presented the question whether law enforcement officials may, without a warrant, search the digital information contained on a smartphone seized in a search incident to arrest.[139] In searching David Riley upon his arrest for driving on a suspended license, the arresting officer found Riley's smartphone in his pocket and looked through it, discovering evidence that Riley had gang connections.[140] The Court had to decide whether the information gleaned from the cell phone was lawfully collected or whether its collection exceeded the scope of the search-incident-to-arrest warrant exception.[141]

Again, the Court—this time in an opinion joined by all nine justices—took the broader view of the Fourth Amendment's protections, pointing to the ways in which new technology changed the analysis on which the search-incident-to-arrest doctrine relied. While smartphones like Riley's were unheard of ten years ago, the Court noted, "a significant majority of American adults now own such phones."[142] Moreover, these phones

137. United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 565 U.S. 400 (2012).

138. Riley v. California, 134 S. Ct. 2473, 2485 (2014).

139. Searches incident to arrest, in which an arresting officer may search the arrestee's person and immediate surroundings to ensure the preservation of evidence and officer safety, are a recognized exception to the warrant requirement. *See* Arizona v. Gant, 556 U.S. 332, 338 (2009) (acknowledging the permissible scope of such searches has long been a source of debate).

140. *Riley*, 134 S. Ct. at 2480.

141. *Id.*

142. *Id.* at 2484.

grant access to "vast quantities of personal information."[143] So while "a mechanical application" of doctrine "might well support the warrantless search," the Court determined that such an application was inappropriate when it comes to smartphones.[144] Permitting such devices to be searched with no warrant would pose a significantly greater intrusion into individual privacy than a traditional search incident to arrest of the nondigital contents of one's pockets.[145]

As with GPS-generated location data, the privacy implications of smartphone data distinguishes it from familiar pre-smartphone contexts not only in volume but also in the nature of the information.[146] A phone with Internet access will have search and browsing history, which could reveal an individual's private interests or concerns—"perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[147] Given the nature of the revelations that searches of smartphone contents permit, the Court determined that individuals have a reasonable expectation of privacy in those contents, even in the course of a valid search incident to arrest.[148]

Less recently, the Supreme Court explicitly recognized the ability of data aggregation to exacerbate privacy concerns in the Freedom of Information Act (FOIA) context.[149] *United States Department of Justice v. Reporters Committee for Freedom of the Press* considered a request under FOIA for a particular individual's criminal record.[150] The Court rejected the request, holding that even though criminal records are publicly available, disclosing a complete rap sheet would be an unwarranted invasion of personal privacy.[151] The Court noted that, "there is a vast difference between the public records that might be found after a diligent search of courthouse files, coun-

143. *Id.* at 2484–85; *see also id.* at 2488 (equating a search of all data stored on a cell phone to a search of an arrestee's wallet or purse was "like saying a ride on horseback is materially indistinguishable from a flight to the moon" because both are ways to get "from point A to point B, but little else justifies lumping them together").

144. *Id.* at 2484.

145. *Id.* at 2488–89.

146. *Id.* at 2489.

147. *Id.* at 2490.

148. *Id.* at 2493.

149. Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (as amended).

150. U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989).

151. *Id.* at 763–70.

ty archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[152] As a result, it reasoned, there is a distinction "between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."[153]

As these cases show, the Supreme Court has already begun to recognize that doctrine must account for the government's technology-enabled ability to glean new kinds of knowledge. Both *Jones* and *Riley*, as well as commentators' suggestions for reforms,[154] however, remain focused on the proper scope of *collection*, trying to calibrate what should be available to the government in the first place. I suggest below that rather than (or in addition to) modifying collection rules, courts should employ *use* restrictions, subjecting some uses of even lawfully collected information to independent Fourth Amendment regulation.

The critical point here is that revelations that the government can glean by querying these databases are different in kind from revelations gleaned by collection alone. That is to say, more data is not necessarily *just* more data. More data can mean *different* data. The aggregation problem means that the right combination of multiple pieces of data can reveal data of an entirely novel—and much more sensitive—nature. So while basic information routinely revealed to the public at large (like momentary location information) may lack constitutional significance, five Supreme Court Justices have indicated that the government's ability to build an individual's profile beyond the scope of what law enforcement agencies would acquire in the absence of the ability to aggregate presents a distinct question.[155]

III. TREATING QUERIES AS SEARCHES

This Article argues that the best way to address the aggregation problem is to reject the idea that the Constitution should remain indifferent to information use. Instead, doctrine should acknowledge that some postcollection and aggregation uses of information qualify as Fourth Amendment events in their own

152. *Id.* at 763–64.

153. *Id.*

154. *See supra* sources cited in note 8.

155. Benjamin J. Priester, *Five Answers and Three Questions After* United States v. Jones *(2012), the Fourth Amendment "GPS Case,"* 65 OKLA. L. REV. 491, 522 (2013).

right. This Part makes the case that some queries of aggregated databases for information about U.S. persons constitute such a use. Section A argues that there some queries violate reasonable expectations of privacy just as surely as some physical searches do, and that those queries should be regulated as searches.[156] Section B offers a means to implement this suggestion by demonstrating that the FISA Court has provided a model for such regulation. Finally, Section C discusses why use restrictions must derive from the Constitution, rather than from statutory or regulatory sources.

Before turning to my argument, however, a clarification is in order: there is a distinction between analyzing large data sets in search of patterns—what is typically referred to as data mining—and querying a data set for information about a particular U.S. person.[157] Retrieving information using query-and-report tools identifies what responsive bits of information a database contains about a specific individual, whereas data mining uses automated processes to discover patterns within the data. My argument applies only to queries. There may be instances when data mining is sufficiently invasive that it, too, should be considered a search; that, however, is a question for another paper.[158]

A. WHY (AT LEAST SOME) QUERIES ARE SEARCHES

As noted above, courts determine what qualifies as a Fourth Amendment search by employing the inquiry first announced in Justice Harlan's seminal concurrence in *Katz v. United States*, which instructs that the Fourth Amendment

156. I take no position here on *how* these searches should be regulated—i.e., whether they should require probable cause and warrants or whether some less demanding standard of review, such as reasonable suspicion, would be appropriate.

157. Data mining is the "process of identifying valid, novel, potentially useful and ultimately understandable patterns in data" or "the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns . . . ." 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(e) (5th ed. 2012) (citations and internal quotations omitted); *see also* Taipale, *supra* note 58, at 37–39 (2003) (noting the difference between data aggregation analyzed with subject-based queries and the use of actual data mining).

158. Imagine, for example, that an algorithm identifies the following pattern: individuals who have both attended services at a mosque and traveled to South Asia are more likely to access terrorist propaganda online. It is not clear whether extracting a list of names of individuals who meet that pattern is any less invasive than a query about a specific individual. I hope to explore this and related questions about other forms of data use in future work.

regulates government activity when it violates an individual's "reasonable expectation of privacy."[159] Like the third-party doctrine, the reasonable-expectation-of-privacy test is subjected to its fair share of criticism, due in large part to its indeterminacy—it is often impossible to divine ex ante whether a court will find that a given set of facts violates a reasonable expectation of privacy.[160] Determining which expectations of privacy are reasonable is therefore more art than science.[161] Yet *Katz* remains the law of the land.

In this Section, I argue that, at the very least, a query constitutes a search if it returns information whose exposure clearly would qualify as a search if that exposure was achieved by collection rather than query. In other words, when queries result in revelations that the Supreme Court has held would violate an expectation of privacy if achieved through collection, that query is a search. In such cases, the reasonable expectation of privacy is no less violated because it was accomplished through a query rather than a more traditional search.

159. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

160. For a representative catalogue of the scholarly critiques of the reasonable-expectation-of-privacy test, see William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1825 n.7 (2016) (collecting articles critiquing the test as ambiguous, subjective, unpredictable, conceptually confused, and circular). As the leading treatise on searches and seizures puts it, the Supreme Court in *Katz* rejected the then-existing, arguably outmoded, Fourth Amendment principles while offering "little to fill the void" it had created. LAFAVE, *supra* note 157 § 2.1(a) ("The Supreme Court . . . has never managed to set out a comprehensive definition of the word 'searches' as it is used in the Fourth Amendment."); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974) (arguing that the question whether something is a search is "a value judgment" regarding how much "privacy and freedom" may be diminished by government surveillance before the Constitution imposes restraints); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007) ("[N]o one seems to know what makes an expectation of privacy constitutionally 'reasonable.'").

161. Of course the Supreme Court has made clear that some collection activities definitively constitute a search. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (finding that the examination of interior of private home with thermal imaging sensor was a search). Conversely, others definitively do not. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 37 (1988) (holding that police examination of contents of an individual's trash left at the curb for collection was not a search); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that police surveillance of private property from a plane in navigable airspace was not a search). For cases that present novel facts, the Supreme Court's eventual outcome is often unclear. *See supra* notes 81–92 and accompanying text (discussing the third-party doctrine).

When queries return information whose collection by other means arguably violates a reasonable expectation of privacy, but the courts have not yet determined whether those means constitute a search, the question becomes more difficult. The government's acquisition of long-term location information about an individual provides a good example. Case law does not clearly indicate whether this acquisition violates a reasonable expectation of privacy and therefore constitutes a search. A query that returns long-term location information by aggregating information from multiple sources—say CSLI, license plate reader records, toll records, and facial recognition paired with surveillance camera footage—therefore may or may not qualify as a search, depending on how the Supreme Court ultimately decides the question. When faced with knowledge acquired by query whose independent collection does not violate a clearly established reasonable expectation of privacy, courts must simply engage in the same analysis that they perform when faced with a new form of collection. They will have to apply the *Katz* test, and make a judgment regarding whether the exposure of that information should be labeled a search. While this leaves uncertainty regarding which queries are permitted, the same is true of new collection methods until the courts resolve their status. When it comes to CSLI, for example, the government has implemented a policy of seeking warrants out of an abundance of caution while we await the Supreme Court's ruling. It could take the same approach to queries whose status is uncertain.

Queries of Section 702–acquired information using U.S. person identifiers present a stark example of the first type of query.[162] Americans unquestionably have a reasonable expectation of privacy in the contents of our electronic communications and to collect them directly the government must first obtain ex ante judicial approval, based on probable cause, in the form of a warrant or a FISC order.[163] Queries seeking U.S. person information in Section 702–aquired information—which includes a "potentially very large" volume of "communications between lawful targets and U.S. persons that are not the type of com-

162. For a description of the Section 702 program, see *supra* notes 70–110 and accompanying text.

163. 50 U.S.C. § 1804 (2012) (discussing foreign intelligence investigations); 18 U.S.C. § 2518 (discussing criminal investigations).

munications Section 702 was not designed to collect"[164] that may "include family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges"[165]—can yield this normally constitutionally protected data with no individualized suspicion, particularity, or ex ante judicial approval.[166] The government thus may "use queries to digitally compile the entire body of communications" associated with an individual, even if that individual is a U.S. person.[167] And in fact, the FBI's internal regulations permit exactly that.[168] Such queries have actually come to be known as the Fourth Amendment's backdoor loophole, because they arguably serve as an end-run around the Fourth Amendment itself.[169] While information about the extent to which the government takes advantage of this "loophole" is imperfect,[170] a FISC judge discouraged Congress from

164. Brief of Amicus Curiae at 11, [Redacted] (FISA Ct., Oct. 16, 2015); *see also* Transcript of Proceedings Held Before the Honorable Thomas F. Hogan at 5–6, *In re* [Redacted] (FISA Ct., Oct. 20, 2015) (arguing that the FBI's rules regarding Section 702 queries "do not provide sufficient safeguards of the U.S. Person information that" Section 702 collects).

165. *Hearing on Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties Before the S. Comm. on the Judiciary*, 114th Cong. 7 (2016) (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board).

166. Professor Laura Donohue has argued that, when used to search for violations of the criminal law, queries of Section 702–acquired material should be considered searches requiring a warrant. Donohue, *supra* note 72, at 262–63.

167. PCLOB SECTION 702 REPORT, *supra* note 71, at 131; *see also id.* at 127 (noting that the privacy implications of Section 702 are not limited to collection, "but must also consider how information about U.S. persons is treated after collection").

168. Memorandum Opinion & Order at 44, [Redacted] (FISA Ct., Nov. 6, 2015).

169. *See, e.g.*, Elizabeth Goitein, *The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider*, JUSTSECURITY (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider. A recent FISC opinion reached the opposite conclusion, determining that queries using U.S. person identifiers did not render the Section 702 program unreasonable for Fourth Amendment purposes. Memorandum Opinion & Order at 77, [Redacted] (FISA Ct., Nov. 6, 2015).

170. PCLOB SECTION 702 REPORT, *supra* note 71, at 130–31 (noting that the FBI "does not separately designate [queries] that employ U.S. person identifiers, and so the number of [such] queries performed by the FBI is not known" making "the manner in which the FBI is employing U.S. person queries . . . difficult to evaluate").

requiring ex ante authorization for such queries because they are so common that the requests would swamp the court.[171]

It is less certain whether the type of query at issue in the Section 215 telephony metadata program or the GPS tracking in *Jones* violates a reasonable expectation of privacy. These types of cases of course present difficult line-drawing challenges.[172] In the Section 215 program, the government (1) collected the metadata of all Americans' phone calls (metadata not subject to Fourth Amendment protections because the government secured it from a third party); (2) combined that metadata into a single database; and (3) then queried that database in search of as-yet-unknown terrorist operatives in the United States.[173] Without the capacity to aggregate these records, the government could acquire Individual *X*'s phone records and learn all of the phone numbers with which Individual *X* communicates.[174] If the government wanted to know more about the communications of people who use the numbers with which Individual *X* is in contact, however, it would have to request individually the records associated with each of the numbers Individual *X* called or from whom Individual *X* received a call. And if it wanted more information about the numbers with which those numbers were in contact, it would have to do the same thing again. A conservative estimate says that two such "hops" would require the government to seek and review records associated with at least 10,000 phone numbers.[175] And if the government expanded the inquiry to three hops, the applicable rule for most of the Section 215 program's history, that number would rise to around 2.5 million.[176] Just as law enforcement is unlikely to follow Mr. Jones's car twenty-four hours a day for several weeks running, intelligence officials are unlikely to un-

171. Letter from Hon. John D. Bates, Dir., Admin. Office of U.S. Courts, to Sen. Dianne Feinstein, Chair, U.S. Senate Select Comm. on Intelligence, at 2 (Jan. 13, 2014).

172. *See* Simmons, *supra* note 22, at 7–8.

173. PCLOB SECTION 215 REPORT, *supra* note 62, at 21–31 (explaining access procedures for foreign intelligence and international terrorism investigations subject to Section 215).

174. *Id.* Section 215 requires only that the information sought be relevant to an ongoing investigation.

175. Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (containing the estimate cited by the court).

176. Noa Yachot, *Writers, Lawmakers, and the NRA Support ACLU Challenge to NSA Spying*, ACLU (Sept. 4, 2013), https://www.aclu.org/blog/national-security/writers-lawmakers-and-nra-support-aclu-challenge-nsa-spying.

dertake this chore on the off chance that they will spot a connection to a known terrorist.

Given a database that includes everyone's phone records, however, one query using Individual *X*'s phone number would return all numbers within the specified number of hops.[177] In one mouse click, the government can discover not only the list of individuals and institutions who were recipients or originators of Individual *X*'s phone calls, but also generate a map of their entire communications network and the networks of everyone with whom they is in contact.[178] Thus, even if we voluntarily relinquish our phone records to our communications provider, as the third-party doctrine assumes, the ability to map our entire social and professional network and what the government may learn from it is far more intrusive than simply gathering a list of numbers with which one person was in contact. Just as five justices believed that using a GPS tracking device to combine data available to the government in unaggregated form violated a reasonable expectation of privacy,[179] so too might this creation of an electronic rolodex violate an individual's expectations of privacy, even if the collection of each individual set of phone records does not.[180] In cases like this, it will not always be clear ex ante when a query will be considered a search. But the same is true of any application of the *Katz* test to novel circumstances.[181]

177. In part for this reason, when Congress renewed Section 215 in the USA FREEDOM ACT of 2015, it barred the government from amassing databases through the bulk collection of records. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861).

178. *See supra* note 161 (referring to a graphics interchange format (GIF) with map showing hops).

179. *See supra* notes 127–29 and accompanying text.

180. One district court implicitly accepted this premise when arguing that the bulk metadata program did not present the same Fourth Amendment question as that of third-party-records cases like *Smith v. Maryland* and should not qualify for the third-party-records Fourth Amendment exemption. *Klayman*, 957 F. Supp. 2d at 31.

181. *See* Kerr, *supra* note 160, at 503 (describing the difficulty in anticipating what constitutes a search under *Katz* as having "disappointed scholars and frustrated students for four decades"). Indeed, judges have reached contrasting conclusions on the question whether the collection aspect of Section 215 constituted a search. *Compare Klayman*, 957 F. Supp. 2d at 31 (holding that bulk telephony metadata should not qualify for the third-party exemption), *with In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted] (FISA Ct., Aug. 25, 2013) (holding that the third-party doctrine applies to bulk telephony metadata).

The issue of aggregating location data provides another example. In *Jones*, several of the justices believed the surveillance violated a reasonable expectation of privacy, and yet the Court did not settle the question whether extended GPS surveillance constitutes a search in the absence of a physical trespass.[182] The Fourth Amendment status of the collection of CSLI remains similarly unsettled.[183] Or imagine a database of all the information gathered by a citywide network of license plate readers. The government could query that database for all cars that ran the red light at the intersection of Main and Broadway. Such a query seems to fall under the *Knotts* rule because it is isolated information about a vehicle's location in a public place.[184] But the government also could query that database for all instances in which it captured the license plate of Jane's vehicle. Like the GPS device in *Jones*, that query could reveal many of the private details of Jane's everyday life by identifying the places that Jane frequents. Just as the *Jones* surveillance arguably violates a reasonable expectation of privacy, so too might the query of the license-plate-reader data. Such queries do not clearly fall on one side of the reasonable-expectation-of-privacy line or the other. Eventually, however, appeals courts will reach a consensus on these specific issues, or the Supreme Court will announce a rule. There is no reason this form of rulemaking, so central to our common law system, cannot be applied to database queries in the same way it is applied to novel questions about information collection.

Another potential objection to this approach is, how will an analyst know, prior to running a query, what information it will return? Since the Fourth Amendment status rests on the nature of the information that the query reveals, rather than the nature of the query itself, it might seem to demand that analysts have a crystal ball enabling them to anticipate whether any particular query will qualify as a search. While this is not an insignificant concern, it can be addressed in a couple of ways. First, there will be times when an analyst running a query will know for sure that the query should be treated as a search. Any query of a database that includes Americans' communications content will, necessarily, implicate a reasonable expectation of privacy. Second, there will be times when an an-

182. *See supra* notes 124–37 and accompanying text (discussing the *Jones* majority and concurrences).

183. *See supra* note 40 (defining CSLI and citing cases).

184. *See supra* notes 93–94 and accompanying text (discussing *Knotts*).

alyst will not know for certain that her query will return Fourth Amendment protected knowledge, but will have a sense—based on the nature of the data being queried as well as the reason for running the query—whether the resulting knowledge will categorize the query as a search. A query of a database with comprehensive historical location data, for example, can be expected to reveal intimate details of the query subject's life akin to those revealed by GPS surveillance in *Jones*.[185] Over time, as the nature of information that certain sets of databases return, it might become much clearer ex ante when a reasonable expectation of privacy is at stake. Finally, it may be that this uncertainty can be captured in the substantive rules that apply to queries that qualify as searches. For example, perhaps such queries qualify as an exception to the warrant requirement, and so the analyst's decision to query must simply be reasonable.[186] Under such a regime, any query that unexpectedly returns information protected by a reasonable expectation of privacy might be considered reasonable nonetheless. Just as the existing application of the reasonable-expectation-of-privacy test presents difficult and often hard-to-predict line-drawing exercises on the part of law enforcement and the courts, so too will determining when queries must be treated as searches (and what limits should be placed on such searches). But just as this has not prevented Fourth Amendment doctrine regarding collection to develop, the same could prove true in the context of information use, such as queries.

To be sure, this rule represents a significant change in conceptualizing the protective scope of the Fourth Amendment. And yet it is no more significant a change than *Katz* itself represented. Prior to *Katz*, *Olmstead v. United States* governed what qualified as a search.[187] Under the *Olmstead* regime, the government did not engage in a search unless it physically intruded into a "constitutionally protected area."[188] Thus in *Olmstead*, installing a tap on telephone wires "did not amount to a search . . . within the meaning of the Fourth Amendment," because the wires themselves were not located in a constitu-

185. *See generally supra* note 98 (discussing the results of the GPS surveillance in *Jones*).

186. *See supra* note 98 (defining reasonableness as an exception to the warrant requirement).

187. 277 U.S. 438 (1928).

188. *E.g.*, Berger v. New York, 388 U.S. 41, 44 (1967).

tionally protected area, like Olmstead's home or office.[189] Over time, however, the Court "departed from the narrow view on which [*Olmstead*] rested," and, finally, in *Katz* explicitly rejected the "constitutionally protected area" formulation in favor of inquiring into "what [an individual] seeks to preserve as private, even in an area accessible to the public."[190] And so was born the reasonable-expectation-of-privacy test.[191]

In rejecting the *Olmstead* approach, the *Katz* majority noted that, "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[192] Similarly, to refuse to acknowledge the expectation of privacy Americans have in the results of some queries is to ignore the technological changes in how information is stored, transferred, collected, and analyzed. If, as *Katz* declared, "the Fourth Amendment protects people, not places,"[193] it should protect them against violations of their reasonable expectations of privacy regardless of the means by which that violation is accomplished. Justice Harlan declared in his *Katz* concurrence that "reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[194] If a wiretap that reveals "what [an individual] seeks to preserve as private" is a search, then a query that exposes that same information represents just as significant an intrusion.[195]

Regulating queries as searches also makes more sense than trying to address this issue by reforming collection rules. To be sure, one can argue that Fourth Amendment harm occurs the moment the government collects information about an individual. When it comes to the type of collection at issue here, we tend to retain our anonymity at the point of collection. Information about our spending or travel habits, or even the content of our Google chats, may be sitting on the government's servers, but nobody is looking at them. To the extent the goal is barring arbitrary government action to protect each individual from unreasonable intrusion into his or her zone of privacy, the moment government action becomes problematic is when it singles

189. 277 U.S. at 466.
190. Katz v. United States, 389 U.S. 347, 352–53 (1967).
191. *Id.*
192. *Id.* at 352.
193. *Id.* at 351.
194. *Id.* at 362 (Harlan, J. concurring).
195. *Id.*

out an individual for scrutiny.[196] Once the government has a particular individual in its sights, it can extract details from the vast ocean of data about that person. And it is at that moment—when the government generates a detailed profile about you from a sea of aggregated data—that Fourth Amendment rules barring arbitrary intrusive action should apply. If we worry about the government extracting information about specific individuals, then the concern manifests itself at the moment of extraction. Addressing the concern at its source also allows us to protect individual rights while continuing valuable collection programs.

There are also technological barriers to relying on collection rules to do all the work. As the President's Council of Advisors on Science and Technology pointed out, data sometimes contains "latent information about individuals," which is revealed only if exposed to certain forms of analysis.[197] One cannot regulate the collection of data one cannot see. Moreover, the aggregation of multiple data points from one form of collection (such as location data) can itself pose problems. Only limiting or eliminating government collection of all location information would address this issue through collection regulation. Finally, it is often impossible to know whether any given data point will reveal intimate knowledge when combined with other data either already in the government's possession or collected subsequently.[198]

A final objection might be that queries hold too much value as an investigative tool to subject to Fourth Amendment limits. Just because some queries constitute searches, however, does not mean government investigators cannot perform them. As the courts often remind us, "the 'touchstone' of the Fourth

196. Solove, *A Taxonomy of Privacy*, *supra* note 10, at 489–90 (recognizing that harms from information use are distinct from those caused by collection). Not only is the collection of large datasets less troubling from an individual rights perspective, it can also be quite valuable. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2–3 (2004) (finding that the government uses data mining to improve service or performance, detect fraud, waste, and abuse; analyze scientific and research information; detect criminal activity, analyze intelligence and detect terrorist activities).

197. PCAST, *supra* note 54, at 39; *see also id.* at x–xi ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy—nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).").

198. *See id.* at 47–48.

Amendment is reasonableness."[199] Just because a query qualifies as a search does not mean the government must secure a warrant based on probable cause. Perhaps it makes sense to include queries in the list of warrant requirement exceptions, such that an analyst running a query must have probable cause to do so but need not secure ex ante judicial sign-off. Or perhaps the courts will consider queries to be more like *Terry* stops,[200] requiring only reasonable suspicion. Courts in this context must be asked to balance the government's interest in law enforcement against society's interests in individual rights, just as they do in so many other places.

B. OPERATIONALIZING QUERY-SEARCHES

Having determined that some database queries are searches—referred to hereafter as query-searches[201]—how can we ensure that the government carries them out in a manner consistent with the Fourth Amendment? To answer this question, this Section first demonstrates that expanding Fourth Amendment protections to some information use is not as radical a departure from existing doctrine as it first might appear. It then details how the FISC has already provided a roadmap for how Fourth Amendment limitations can be imposed on database query-searches.

1. The Foundation for Constitutionally Based Use Restrictions

While the Constitution is silent on the government's use of information in the lion's share of circumstances,[202] the Fourth Amendment does, in fact, require more than the traditional constitutional protections governing searches and seizures in a handful of situations. Both Congress and the courts consider some information collection methods so intrusive that postcollection constraints on information use are necessary.[203] So, in some ways recognizing queries as potential searches merely expands existing doctrine rather than contradicting it.

199. *E.g.*, Ohio v. Robinette, 519 U.S. 33, 39 (1996).

200. *See supra* note 98 and accompanying text (discussing *Terry v. Ohio*, 392 U.S. 1 (1968)).

201. To make plain, when I am referring to queries that should be considered Fourth Amendment searches, I refer to them as query-searches.

202. *See supra* Part II.B.

203. *See generally* S. REP. NO. 95-701 (1978) (discussing the constraints on information use for collection methods); *see also* Berger v. New York, 388 U.S. 41 (1967) (stating that wiretapping must have limitations in order to adhere to the Fourth Amendment).

Nearly fifty years ago, concerns regarding the intrusive nature of wiretapping prompted the Supreme Court to augment the Fourth Amendment's typical warrant requirements (probable cause, particularity, and review by a neutral magistrate) with procedural rules about how the government handled the information it collected using that tool.[204] The Supreme Court's ruling made it plain to Congress that, to satisfy constitutional demands, any use of wiretapping must include information handling limits.[205] Thus when enacting legislative authorization for wiretapping, Congress included such limits, known collectively as minimization procedures.[206] Minimization procedures regulate the government's handling of information so as to mitigate the risks that electronic surveillance poses for Americans' individual privacy rights.[207] The statutes authorizing wiretapping for both domestic law enforcement and foreign intelligence purposes require minimization.[208] While criminal investigations implement minimization requirements at the moment of collection,[209] FISA requires minimization in the retention and dissemination of information as well in order to ensure "information concerning American citizens and lawful resident aliens be handled in such a way as to assure that it is used only for the purposes specified."[210] The constitutional need to minimize information has, over time, expanded beyond the wiretapping context and currently applies to collection of tan-

204. 388 U.S. 41 (1967).

205. *Id.*

206. *See, e.g.*, United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) (citing S. REP. NO. 95-701, at 13 (1978)) ("FISA reflects both Congress's 'legislative judgment' that the court orders and other procedural safeguards laid out in [FISA] 'are necessary to insure that electronic surveillance . . . conforms to the fundamental principles of the fourth amendment [sic].'"); Berman, *supra* note 33, at 791–817 (discussing constitutional origins of minimization procedures); Donohue, *supra* note 72, at 220 ("FISA was Congress's express decision to curb executive power as a constitutional matter.").

207. 50 U.S.C. § 1801(h) (2012) (defining minimization procedures); PCLOB SECTION 702 REPORT, *supra* note 71, at 50 (asserting that minimization procedures impose a "set of controls on data" to "balance privacy and national security interests").

208. 18 U.S.C. § 2518(5) (every wiretap order "shall contain a provision that the authorization to intercept shall be . . . conducted in such a way as to minimize the interception of communications not otherwise subject to interception"); 50 U.S.C. §§ 1804, 1805 (requiring government surveillance applications and FISC authorization orders to include minimization procedures).

209. S. REP. NO. 95-701, at 41 (1978) (stating that criminal procedures are an exception to the minimization rule).

210. S. REP. NO. 95-604, at 38 (1977).

gible things, physical searches, and collection of communications metadata.[211]

The requirement to minimize is imposed statutorily; the task of determining exactly what minimization should look like in any particular circumstance, however, is left to the courts.[212] Minimization procedures thus represent a mandate to courts to include limits on what the government may do with information gleaned from at least some forms of collection.

At times, courts have also imposed limits on the government's use of lawfully collected information even in the absence of a legislative requirement.[213] Recently, for example, the FISC considered whether the FBI's queries using U.S.-person selectors should be treated as searches subject to Fourth Amendment regulation.[214] While the court ultimately rejected the idea that such queries were themselves searches, it did not find them irrelevant to the constitutional analysis.[215] Instead, the use to which the government plans to put information collected under Section 702, the FISC concluded, should form part of the assessment of the reasonableness of the Section 702 program as a whole.[216] So while the FISC did not impose Fourth Amendment constraints directly on queries as such, it recognized the constitutional concerns that can arise out of some uses of information.[217]

Postcollection use has also become an issue for computer searches. Because it is often not feasible to identify and isolate computer files responsive to a warrant at the time of seizure, it is common practice to make identical copies (or mirrors) of

211. *See* 50 U.S.C. § 1861(b)(2)(D) (collection of tangible things); *Id.* § 1881(a) (collection of electronic communications by targeting non-U.S. persons overseas); *Id.* § 1823(a) (physical searches for foreign intelligence purposes). Collection using a pen register or trap-and-trace device, which provides information about incoming or outgoing communications, now must employ "privacy procedures," which are simply minimization procedures by another name. *Id.* § 1842(h). *See* Berman, *supra* note 33, at 790–817. (providing a history of the evolution and development of minimization procedures).

212. Surveillance laws have consistently assigned the job of determining what minimization procedures are appropriate to the courts. 50 U.S.C. §§ 1805(a)(3), 1861a(1).

213. [Redacted] Memorandum and Opinion & Order at 41 (FISA Ct., Nov. 6, 2015); *id.* at 40 (rejecting the argument that "each query of Section 702–acquired information [using U.S.-person identifiers] is a 'separate action subject to the Fourth Amendment reasonableness test'").

214. *Id.*

215. *Id.* at 42.

216. *Id.* at 40–41.

217. *Id.* at 41–45.

computer hard drives to review their contents off-site.[218] In so doing, however, the government necessarily seizes a great deal of nonresponsive material—everything on the computer drive unrelated to criminal activity, such as family photos, contact lists, emails, and the like. Courts have recently grappled with how to limit the government's access to or use of that nonresponsive information. In *United States v. Ganias*, for example, the court considered whether investigators can obtain a warrant to search a set of files the government happens to have in its possession because they were seized pursuant to a previous warrant, to which those files were not responsive.[219] A three-judge panel of the Second Circuit held that despite the valid initial collection of the information, the government violated the defendant's Fourth Amendment rights by retaining the nonresponsive information in the absence of "some independent basis" for doing so.[220] Permitting the government to "retain all the data on [an individual's] computers on the off chance the information would become relevant to a subsequent criminal investigation," the court said, would "be the equivalent of a general warrant."[221] And in his concurring opinion in *In re Comprehensive Drug* Testing, Judge Alex Kozinski articulated a list of suggested guidelines for investigators to follow when executing searches that are likely to expose investigators to nonresponsive information.[222]

218. This two-step process of first seizing or copying digital storage devices and then searching its contents later is routine. *See* FED. R. CRIM. P. 41(e)(B).

219. 755 F.3d 125, 138 (2d Cir. 2014), *vacated on other grounds*, 824 F.3d 199 (2d Cir. 2016).

220. 755 F.3d at 138. The Second Circuit subsequently agreed to hear the case en banc, vacated the panel decision, and resolved the case on other grounds, declining to rule on the validity of the data retention or the second warrant. The en banc court did recognize, however, the highly intrusive nature of the government's actions, observing that "the seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." *Id.*

221. *Id.* at 137; *accord* United States v. Weikert, 504 F.3d 1, 17 (1st Cir. 2007) (recognizing that "there may be a persuasive argument . . . that an individual retains an expectation of privacy in the future uses of her DNA profile").

222. United States v. Comprehensive Drug Testing, Inc., 621. F.3d 1162, 1178–80 (9th Cir. 2010) (en banc) (Kozinski, J., concurring). Some magistrate judges have also begun imposing limits on how the government executes searches of digital storage devices. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010) (noting this

These isolated instances, while representing a tentative extension of Fourth Amendment rules into the use space in certain contexts, do not go far enough. Each of these examples represents what I call a collection-plus regime. Either Congress or the courts determine that collection rules alone are insufficient, so they augment those rules with use restrictions. Numerous commentators have also advocated some form of collection-plus regime, where postcollection use of information is considered relevant to the constitutionality of the original search or seizure.[223] A collection-plus regime does not independently require use constraints, but instead applies them cumulatively, adding their procedural protections to those of the collection rules. The question is thus whether the whole of the government's action, from collection to use, complies with Fourth Amendment demands.

These collection-plus approaches take a step in the right direction by recognizing that the government's postcollection use, at least in certain circumstances, is constitutionally relevant. I contend, however, that collection-plus regimes do not go far enough. The most critical shortcoming of collection-plus is

practice and arguing that it is both unwise and beyond the scope of the magistrates' power).

223. *See, e.g.*, Deven R. Desai, C*onstitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 625 (2014) (arguing for time limits on the use of data); Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 720 (2014) (advocating further development of use restrictions); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 25 (2015) ("Although the seizure of nonresponsive files is reasonable when needed to effectuate the search for responsive files, subsequent use of the seized nonresponsive files transforms the nature of the seizure and renders it constitutionally unreasonable."); Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendmen*t, 74 TEX. L. REV. 49, 51 (1995) (arguing that "the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information"); Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J.F. 8, 15–16 (2016) (arguing that courts assessing the constitutionality of government action should take into account "not only the nature of the data the government is collecting, but the use the government is going to make of that data"); Peter Swire, *A Reasonableness Approach to Searches After the* Jones *GPS Tracking Case*, STAN L. REV. ONLINE, Feb. 2012, https://www.stanfordlawreview.org/online/privacy-paradox-a-reasonableness-approach-to-searches-after-the-jones-gps-tracking-case (arguing that factors such as the length and intrusiveness of surveillance as well as the use of minimization procedures, if any, should factor into the question whether the government search was reasonable); *cf.* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 388 (2015) (noting that acquisition and use restrictions "must go hand-in-hand").

that when it comes to Fourth Amendment–exempt information—such as third-party records—there is no constitutional analysis into which one could incorporate limits on the government's postcollection use.[224] For all the vast spectrum of information, ranging from the innocuous to the intensely private, that is exempt from Fourth Amendment coverage, courts have no opportunity to consider whether the use of that information renders its collection unreasonable, because the Fourth Amendment's reasonableness requirement does not apply in the first place.[225] Moreover, it is not clear at the time of collection whether or when the aggregation problem will arise with respect to particular data. The insight that aggregation permits may result only from the combination of data sets that are fused after—perhaps years after—the collection has taken place.[226] The idea of assessing the government's action as a whole in those circumstances is unwieldy at best. If you accept the argument that queries of aggregated information reveal more than the individual bits of information the government collects, we must recognize those uses themselves as searches entitled to their own independent Fourth Amendment analysis, regardless of how the underlying information was collected.

2. Implementing Query-Search Limits

If one accepts the argument that courts should assess query-searches independently of the means by which the information was collected, the question becomes how they might do so. Here, I argue that the FISC has already shown us what such an analysis might look like. Indeed, the minimization procedures that FISC judges demanded in their orders approving

224. Donohue, *supra* note 72, at 243 (describing Professor Kerr's argument that "because third-party record collection constitutes neither a search nor a seizure, the doctrine would have to be radically overhauled to make all collection of data a seizure to then trigger a reasonableness analysis").

225. United States v. Knotts, 460 U.S. 276 (1983) (holding that it is neither a search nor a seizure to monitor the location of a beeper placed in chemicals being transported to owner's cabin); Smith v. Maryland, 442 U.S. 735 (1979) (holding that a telephone company's use of a pen register is not a search); Hoffa v. United States, 385 U.S. 293 (1966) (holding that testimony from conversations between government informant and defendant did not violate the search and seizure limits of the Fourth Amendment). *But see* United States v. Karo, 468 U.S. 705 (1984) (holding it is a search to monitor a beeper that is inside a house and therefore withdrawn from public view).

226. *See* PCAST, *supra* note 54 at ix; *id.* at xii (noting that collection rules cannot guard against future, unknown privacy threats, so use is "the technically most feasible place to protect privacy").

the Section 215 bulk metadata collection program look more like the Fourth Amendment warrant requirement procedures than anything else.[227] The Section 215 program itself was not subject to Fourth Amendment limits because the government argued, and the FISC agreed, that the metadata collection fell within the scope of the third-party doctrine.[228] The statutes required minimization procedures, but given the absence of Fourth Amendment demands, such procedures could have been nominal. As I have argued elsewhere, in imposing robust limits on query-searches of the Section 215 database nonetheless, the FISC signaled recognition of those query-searches' Fourth Amendment–based implications and demonstrated how other, similarly intrusive query-searches might be subject to Fourth Amendment oversight.[229]

Before demonstrating this point, a quick primer on the purposes of each of the warrant requirement's three elements is in order. First, there is ex ante review by a neutral magistrate, based on the idea that officials with "investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means . . . . The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain" information and "overlook potential invasions of privacy and protected speech."[230] Second, the cause requirement limits arbitrary government action.[231] In forcing the government to demonstrate that there is an answer to the question why are you searching this person or seizing this information?, cause requirements guarantee that the search or seizure will be based on objective evidence, rather than the exercise of unfet-

227. *See infra* notes 234–39 and accompanying text. For a detailed discussion of the Section 215 use regime and its constitutional shadings, see Berman, *supra* note 33, at 806–17.

228. *See In re* [REDACTED], No. PT/TT [REDACTED] (FISA Ct., July 14, 2004). The limits on the collection of that data were statutory: the information had to be both "relevant" to an authorized terrorism or intelligence investigation and subject to minimization procedures. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1861(b) (2015).

229. *See* Berman, *supra* note 33, at 817–24.

230. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 317 (1972).

231. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 317 (2016) ("[T]he sine qua non of official arbitrariness is allowing officers unfettered 'discretion' to search whenever the whim strikes."). Individualized suspicion requirements reduce the likelihood of government intrusion on the basis of (implicit or explicit) bias, individual animus, or other improper motives. *Id.* at 317–20.

tered executive discretion.[232] Third, the particularity requirement prevents the government from "rummag[ing] through homes in an unrestrained search for evidence of criminal activity."[233] So just as the government must explain why it has singled out a particular individual, it must also explain exactly what it expects the search to yield. Together, these requirements ensure that a government determination to intrude into an individual's private realm is both objectively justified and limited in scope.

The FISC imposed approximations for each of these elements in its oversight of the Section 215 program. First, it required all queries to be approved through ex ante review by a high-ranking government official. If the query-search involved "seed accounts . . . used by U.S. persons," approval had to come from the NSA's Office of General Counsel (NSA OGC).[234] So while individual determinations regarding whose metadata would be accessed did not require *judicial* preapproval, the NSA OGC's approval did serve to diminish discretion by ensuring that officers with "investigative and prosecutorial duty" were not "the sole judges" of when to execute queries about U.S. persons.[235] While someone in the NSA's OGC is not an independent magistrate, she is more able to make an impartial assessment than an agent or official actually involved in an investigation.

Second, the FISC imposed a cause standard on Section 215 query-searches, in the form of the "reasonable articulable sus-

232. When the courts have not insisted on individualized suspicion, they have usually insisted on some other means of limiting the discretion of the officers in the field. *See* Delaware v. Prouse, 440 U.S. 648, 654–55 (1979) (holding that when the circumstances preclude "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'" (quoting Camara v. Mun. Court, 387 U.S. 523, 532 (1967))); Friedman & Stein, *supra* note 231, at 310 (quoting Brown v. Texas, 443 U.S. 47, 52–53 (1979)). *But see* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 278–79 (2011) (arguing that the special needs doctrine permits suspicionless searches with no limits on discretion).

233. Riley v. California, 134 S. Ct. 2473, 2494 (2014) (citations omitted) (pointing out that "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' . . . of the colonial era," which permitted indiscriminate searches).

234. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 06-08, 6 (FISA Ct., Aug. 18, 2006).

235. *Id.*

picion" requirement.[236] This standard required a determination that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion (RAS) that [the particular seed] to be queried is associated with [REDACTED—probably 'an international terrorist organization' or 'Al Qaeda']."[237] The FISC actually saw the reasonable articulable suspicion standard as analogous to a cause requirement, asserting that imposing this limit on query-searches would ensure "that '[t]he information actually viewed by any human being . . . will be just as limited—and will be based on the same targeted, individual standards'" as searches governed by the Fourth Amendment.[238]

Finally, the reasonable articulable suspicion standard steps in for the particularity requirement as well. That collection of everyone's telephone metadata will net a huge amount of irrelevant information is a certainty.[239] Because query-searches could be directed only at those seed identifiers for which the government had reasonable articulable suspicion of connection to a terrorist organization, however, the government is limited to inquiries that will yield information related to the communications of suspected terrorists and their associates. Government officials could not query the database in search of nonterrorism-related crimes or threats.

These minimization requirements are not identical to the ones that would apply to the collection of information whose seizure required a warrant. But they do create proxies for each of those traditional protections. The FISC thus employed minimization rules to impose limitations that clearly took Fourth Amendment concerns into account.

3. Implications for Surveillance Programs and Beyond

Query-searches could be subjected to a regime similar to the one the FISC imposed on the Section 215 program.[240] This

236. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-80, 3 (FISA Ct., Apr. 25, 2013).

237. *Id.* No U.S.-person seed could meet the RAS standard solely on the basis of activities protected by the First Amendment. *Id.*

238. *In re* [REDACTED], No. PR/TT [REDACTED], 58 n.41 (FISA Ct., July 14, 2004) (internal quotations and emphasis omitted).

239. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, 18 (FISA Ct., Aug. 29, 2013).

240. This Article does not advocate interpreting the Fourth Amendment to require for all query-searches the exact same rules that the FISC imposed in

is perhaps most compelling in the context of querying Americans' Section 702–acquired communications, which includes the contents of U.S. persons' communications with overseas targets. The government takes advantage of the absence of constitutional limits to query-search Section 702–acquired information using selectors associated with U.S. persons, thereby gaining access to the contents of Americans' communications with no individualized suspicion, no particularity requirement, and no ex ante review. Hence the "backdoor loophole" moniker by which such query-searches are known.

Unfortunately, the FISC rejected the argument that these queries should be treated as searches, instead holding that they should be subject to a collection-plus regime.[241] According to the FISC opinion, the queries are not themselves searches, but their use must be factored in to the constitutionality of the Section 702 program as a whole.[242] But the constitutionality of the government's access to U.S. persons' communications content should not be dependent on how other aspects of the Section 702 program operate. Access to Americans' communications content is at the heart of traditional Fourth Amendment protection. The same rules should apply whether the government accesses that information from a database sitting on its own servers, secures a warrant to acquire that information from a communications provider's server, or executes a warrant to seize an individual's personal computer. Section 702 query-searches should be considered reasonable only when the government can demonstrate to an executive branch official, or (even better) to the FISC itself, individualized suspicion about the target of the query-search.[243] Moreover, a particularity requirement should limit the government to query-searches that are designed to return information relevant to the purpose of the program—foreign intelligence information. This would allow the government to both continue employing Section 702 for its original purpose—the collection of foreign intelligence—and prevent the use of U.S.-person identifiers to access communica-

the Section 215 program. Once queries are recognized as searches, reasonable minds can disagree regarding what those rules should be; I defer to another day the difficult task of answering that question.

241. *See supra* notes 216–17 and accompanying text.

242. *Id.*

243. The USA FREEDOM Act of 2015 requires the government to seek FISC approval for any queries of telephone metadata. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861 (2012)).

tions to which it would not have lawful access in the absence of Section 702.

Query-searches are not limited to the foreign intelligence context. Government officials of all types utilize databases to seek out information about U.S. persons. In fact, before even opening an official investigation, FBI agents are authorized to examine not only all FBI and Department of Justice records, but also "records maintained by . . . other federal, state, local, or tribal, or foreign governmental entities or agencies."[244] Such inquiries require an "authorized purpose," but no individualized suspicion.[245] This authority may be used to obtain information "on individuals, groups, or organizations of possible investigative interest," either because they may be involved in crime or threats to the national security "or because they may be targeted for attack or victimization."[246] Thus federal agents have a green light to query any and all databases available to them about U.S. persons even in the absence of individualized suspicion.

Queries of government databases by federal, state, local, or tribal law enforcement entities can prove just as intrusive as those used in the Section 215 or Section 702 programs. The NYPD's DAS, for example, can track where a particular car is located and where it has been the past days, weeks, or months and it can aggregate that information with license plate information, as well as watch lists and criminal history.[247] In other words, it allows the police to identify connections between persons, places, and things in ways that a human crime analyst may not have been able to do.[248] Cross-referencing the federal government's biometric databases with surveillance camera footage or photos on social media websites could provide an hour-by-hour account of a particular individual's location and activities.[249] Imagine a query compiling financial records with information about products with RFIDs. Such a query would

244. FED. BUREAU INVESTIGATIONS, THE ATTORNEY GEN.'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 20 (2008).

245. Authorized purposes are "to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence." *Id.* at 19.

246. *Id.* at 17.

247. *See* Joh, *supra* note 11, at 48–49.

248. *Id.*

249. *See* Jennifer Lynch, *FBI's Facial Recognition Is Coming to a State Near You*, ELECTRONIC FRONTIER FOUND. (Aug. 2, 2012), https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you.

indicate what one purchases and where (or to whom) it goes. Similarly, combining employment records with travel records could expose the fact that your last sick day was actually a three-day weekend at the beach.

Sometimes database queries will be highly effective tools used to locate criminals, and this Article does not argue that the government should be barred from using them wholesale. Instead, the argument is merely that when the government uses a U.S.-person identifier to search aggregated information, that query should often qualify as a search and the Constitution should impose limits on those queries, just as it does a search of your home or a stop-and-frisk on the street.

C. THE INDISPENSABILITY OF CONSTITUTIONAL REGULATION

The foregoing discussion has largely focused on what the *Constitution* requires or permits. But, of course, the Constitution is not the only means of regulating government conduct. Many of the government's collection techniques (as well as some uses) are subject to statutory, regulatory, or policy-based limits. Here, I explain why these existing nonconstitutional rules do not sufficiently address the concerns raised by query-searches, and will not likely do so in the future.

Those who are content to rely on legislative or regulatory action to impose limits on the government's use of new technologies argue that policy makers are better suited than courts to determine appropriate constraints.[250] Congress's past performance in regulating to protect privacy, however, does not support this approach. Legislative measures addressing perceived shortcomings in data privacy are almost universally perceived as outdated, incomplete, insufficiently rigorous, or some combination of the three.[251] The United States lacks an overarching,

250. *E.g.*, Kerr, *supra* note 121, at 857–81 (arguing that courts do not respond to new technological challenges swiftly enough and that we should rely on the legislature to do so instead); Peter Margulies, *Searching for Judicial Power: Article III and the Foreign Intelligence Surveillance Court* (Roger Williams Univ. Sch. of Law, Working Paper No. 171, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2827767 (arguing that Congress should be given deference in making decisions related to national security and evolving technology). *But see, e.g.*, Swire, *supra* note 81, at 915–19 (expressing skepticism regarding Congress's ability to protect privacy effectively).

251. *See, e.g.*, Solove, *Access and Aggregation*, *supra* note 36, at 1154 ("Our information regulatory infrastructure is disconnected, often outdated, and inadequate to meet the challenges of the new technologies of the Information Age."). ECPA requires a warrant for collecting the contents of your e-mail, but

unified information protection regime. Instead, when Congress has acted at all, it has done so piecemeal, through a series of narrowly targeted statutes.[252]

The USA Freedom Act of 2015 might initially paint a promising picture.[253] After all, the FISC did impose Fourth Amendment–like minimization procedures on the Section 215 program,[254] the reauthorization debate as the statute approached its sunset date was intense, and Congress ended up codifying, in large part, the FISC's judicially imposed limits on Section 215's scope.[255] Indeed, one provision in the legislation

not for collecting other data stored in the cloud. *See, e.g.*, Kerr, *supra* note 90, at 1213–18.

252. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1430–45 (2001) [hereinafter Solove, *Privacy and Power*] (discussing the "limits of privacy law" and identifying flaws in multiple privacy statutes, including those protecting information about credit records, health, and education, as well as information included on drivers' licenses and in electronic communications); Taipale, *supra* note 58, at 53–55 n.223 (comparing the piecemeal U.S. information privacy regime with Europe's more comprehensive approach); Solove, *Privacy and Power*, *supra*, at 1440 ("Since the 1970s, Congress has grappled with the problem of databases, but has been slow to take action."). Moreover, when statutory protections do apply, those "protections" are much less rigorous than typical Fourth Amendment rules, often dispensing with ex ante review or individualized suspicion. Solove, *Privacy and Power*, *supra*, at 1430–45. Statutory limits often set a low threshold for the government to meet. *E.g.*, Stored Communications Act, 18 U.S.C. § 2703(d) (2012) (information must be "relevant and material to an ongoing . . . investigation"); *Id.* § 2703(d) (requiring "specific and articulable facts" (but not probable cause) giving reasonable grounds to believe the information will be relevant and material to an ongoing investigation). Most information in the hands of third parties may be acquired simply by issuing a subpoena, some of which may be issued by prosecutors or law enforcement officials with no prior judicial approval. *E.g.*, *id.* § 3486 (administrative subpoenas); *id.* § 2709 (national security letters, which permit the FBI to get customer's telephone toll and transactional records); *see also* 12 U.S.C. § 3414; 15 U.S.C. § 1681u (banking, financial, and credit information).

253. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified at 50 U.S.C. § 1861) (barring bulk collection of telephone and Internet metadata). As I have argued elsewhere, the USA FREEDOM Act was a shift in the right direction, but it did not do nearly enough. *See* Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 IND. L.J. 1191 (2016).

254. *See supra* notes 234–39 and accompanying text.

255. In modifying the Section 215 authorities in the USA FREEDOM Act of 2015, Congress retained many of the limits initially imposed as minimization procedures by the FISC. The legislation preserved the individualized cause requirement by codifying the RAS standard. 50 U.S.C. § 1861(b)(2)(C) (to access calling records the government must show "there is a reasonable, articulable suspicion" that the seed identifier—the "special selection term" (SST) in the language of the statute—"is associated with" a foreign power or an agent of a foreign power "engaged in international terrorism"). The statute also in-

was even more restrictive than the one the FISC required, perhaps because some legislators argued the Constitution demanded it.[256] Thus we had a regulatory regime that was adopted, refined in part due to constitutional concerns, and codified by Congress. Problem solved, right? Wrong.

To the extent the USA Freedom Act is a success story, it is the exception, not the rule. As an initial matter, the prior version of Section 215 had a sunset date. And while sunsets alone are not usually sufficient to force policy changes, this sunset provision followed closely on the heels of Edward Snowden's massive leak of information about U.S. surveillance activities.[257] That leak revealed that the government was interpreting Section 215 of FISA in an expansive and highly controversial way. In other words, the revelation of a secret program, targeted at Americans, and interpreting executive collection powers in the most aggressive way possible was enough to prompt Congress to restrict query-searches in that context. By contrast, Section 702 sunsets on December 31, 2017, yet there has been no public outcry objecting to the way the government query-searches the communications of Americans scooped up that program. Some legislators believe that such query-searches violate the Fourth Amendment, but that view has not led to change, nor does it seem likely that it will.[258]

cluded a particularity requirement. *Id.* §§ 1861(k)(4)(B), 1861(c)(2)(A) (allowing collection regarding only an SST that "specifically identifies an individual, account, or personal device" and requiring that the FISC's order describe "each specific selection term . . . with sufficient particularity to permit them to be fairly identified"). The statute's ex ante review requirement differed from the FISC's Section 215 minimization rules in that it requires prior review by the FISC itself rather than internal executive branch officials. *Id.* § 1861(a).

256. *E.g.*, 161 CONG. REC. H2916 (daily ed. May 13, 2015) (statement of Rep. Nadler) ("[T]he dragnet collection without a warrant of telephone records . . . is the contemporary equivalent of the British writs of assistance . . . that the Fourth Amendment was drafted to outlaw."); 161 CONG. REC. H2920 (daily ed. May 13, 2015) (statement of Rep. Jeffries) ("[E]nding bulk collection through section 215" was a step toward "restoring the balance" between effective national security and respect for privacy demanded by the Constitution).

257. *See* Emily Berman, *The Paradox of Counterterrorism Sunset Provisions*, 81 FORDHAM L. REV. 1777 (2013) (arguing that sunsets fail to prompt legislative reform unless they coincide with a scandal of some kind).

258. *E.g.*, 161 CONG. REC. E726-04 (2015) (statement of Rep. Sensenbrenner) ("Section 702 of FISA has been improperly used to obtain the content of Americans' private communications without a warrant, which is unconstitutional under the Fourth Amendment."); 161 CONG. REC. H2923 (daily ed. May 13, 2015) (statement of Rep. Sanford) ("'The notion that Americans' rights are contingent on the geography of where a call is directed is not consistent with the Constitution and highlights why [Section 702] needs to be changed.").

The perfect storm that swept the USA Freedom Act into existence is not something we can count on happening regularly. The Snowden leaks are likely a once-in-a-generation event. The only comparable historical event is the leak of the Pentagon Papers half a century ago. The Snowden leaks not only triggered sufficient outrage regarding Section 215 to motivate legislative action; they also brought to light the very existence of the program. If Congress or the American public are not aware of the way the government is using information, legislative action is impossible. Thus the FBI's efforts to keep its use of Stingrays under wraps ensured that the public lacked sufficient information to generate or enable opposition by legislators or their constituents. Nor do most people know whether and how their state or local law enforcement agencies employ information gathered from Stingrays, license plate readers, surveillance camera footage, or other modern collection methods.

Congress's efforts to fill perceived statutory holes in the privacy regime, when they do come, have sometimes stalled indefinitely. For years, there has been bipartisan consensus, for example, that the Electronic Communications Privacy Act needs to be updated to reflect current technology.[259] The Email Privacy Act, a reform bill, passed the House of Representatives 419–0.[260] Yet it still languishes, caught up in debate over when the government will be able to access information protected by the law.[261]

Reliance on regulatory regimes imposed on query-searches through minimization requirements warrants similar skepticism. First, foreign intelligence collection is effectively the sole context to which minimization requirements apply. Among all of the domestic law enforcement tools, only the law regulating wiretaps requires the government to minimize. And there, minimization applies only to the collection stage, rather than the retention, use, and dissemination stages that dominate FISA

259. James Stiven, *ECPA Reform Will Protect Privacy and Meet Law Enforcement Needs*, HILL (June 2, 2016), https://www.thehill.com/blogs/pundits-blog/technology/281987-ecpa-reform-will-protect-privacy-meet-law-enforcement-needs (noting that "[f]ew problems in recent years have drawn more extensive bipartisan support" than ECPA reform).

260. Email Privacy Act, H.R. 699, 114th Cong. (2015); H.R. REP. NO. 114-528 (2015).

261. Marcy Wheeler, *Why Is the Government Poison-Pilling ECPA Reform?*, EMPTYWHEEL (June 7, 2016), https://www.emptywheel.net/2016/06/07/why-is-the-government-poison-pilling-ecpa-reform.

minimization.[262] Moreover, minimization in the criminal context sometimes seems to be more honored in the breach, thanks in part to the Supreme Court's reluctance to suppress evidence based on failure to minimize.[263] If the Fourth Amendment applied to all query-searches, courts would be required to impose necessary constraints in all areas of law, not just in wiretaps and foreign intelligence surveillance.

Second, minimization procedures apply only to information not available publicly. Depending on how broadly the concept of public information is construed, this could include a great deal of the information that the government collects under Fourth Amendment exemptions or purchases from third parties. Yet, as *U.S. Department of Justice v. Reporters Committee for Freedom of the Press* recognized, the aggregation of publicly available information can be quite revealing.[264]

Third, one common means of minimizing data is to strip out any personally identifying information.[265] As more and more information becomes available, however, rediscovering the personally identifiable information, even after it has been stripped is relatively easy to do. Some attributes are uniquely identifying on their own, but more importantly any attribute can be identifying in combination with others. One study showed that by combining "public, Personal Genome Project profiles containing zip code, birthdate, and gender with public

262. *See* Berman, *supra* note 33, at 790–99.

263. *See* Scott v. United States, 436 U.S. 128, 139–42 (1978) (holding that the failure of agents executing a wiretap warrant to make a good faith effort to minimize interception did not require suppression); James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Law To Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 77 (1997) ("The minimization requirement . . . has not been strictly enforced . . . ."); Peter J. Georgiton, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831, 1860 (2001) ("The [*Scott*] Court's determination of what factors constitute 'reasonableness' for the purposes of minimization requirements has been applied by lower courts to justify a variety of broad searches.").

264. *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763–64 (1989).

265. Personally identifiable information is

> information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., U.S. Office of Mgmt. & Budget to the Heads of Exec. Dep'ts & Agencies, M-07-16 n.1 (May 22, 2007).

voter rolls, and mining for names hidden in attached documents, 84–97 percent of the profiles" could be accurately matched with a name.[266] As technology advances, minimization practices like anonymization and data deletion that have been used for privacy protection in the past are not going to work because they are "increasingly easily defeated by the very techniques" that are used in analyzing data.[267]

Finally, another crucial difference between constitutional doctrine and the implementation of statutes and regulations is their transparency. Another lesson Edward Snowden taught us is that knowing the language of the statute is not always sufficient to understand exactly how that statute is being implemented. Rules that impact fundamental rights like privacy should be entirely public.[268] Too often, agency interpretations, guidelines, targeting and minimization procedures, and other limits originating in the executive branch have remained secret. This is not the case when it comes to judicial opinions, and to the extent the rules are developed by the FISC (whose decisions often are classified), any statutory or constitutional interpretation that court engages in also must be made public.

Since neither statutory nor minimization-based constrains will successfully alleviate concerns regarding the intrusiveness of query-searches, Constitution-based rules must be developed. To be sure, such rules will impose costs and burdens on government agencies and officials, potentially reducing investigative efficiency. On the other hand, forcing government officials to target only those individuals for whom individualized suspicion exists could improve efficiency, eliminating fruitless fishing expeditions. More importantly, however, not all limits on government activity are designed to maximize efficiency. Rather, some are there to protect individual rights, even if such protection renders governance incrementally less efficacious.

CONCLUSION

Throughout the nation's history, changes in the technology to which the government has access when conducting investigations have prompted adjustments in legal doctrine. Today as

266. PCAST, *supra* note 54, 39–40.

267. *Id.* at xi, 38.

268. *See generally* Dakota S. Rudesill, *Coming to Terms with Secret Law*, 7 HARV. NAT'L SEC. J. 241 (2015) (arguing against the idea of secret law and in favor of a presumption that the rules available to the public accurately inform the polity of what the government is doing).

never before, technology has steamed ahead at a pace with which the law has struggled (unsuccessfully) to keep up. Today's technology provides not only better versions of existing tools; it also provides entirely new tools, tools that do not fit neatly into any of our doctrinal paradigms. The government has gone from building profiles on individuals by seeking out paper files from disparate sources in various jurisdictions to aggregating massive amounts of data with the click of a mouse. This capacity to aggregate information, when combined with the amount of detailed information about each of our lives that is digitally captured and preserved, is not just a better mousetrap; it is a global mouse vaporizer. That is to say, it must be recognized as a new phenomenon, not merely a more effective version of an existing tool. While the phenomenon is new, the red flags it raises are as old as government itself. Fortunately, our founding document speaks not in the language of technology but in the language of rights. And those rights must be preserved even in the face of an information revolution in a digital age. When queries of aggregated information reveals knowledge in which U.S. persons have a reasonable expectation of privacy, the Fourth Amendment right to be secure in our persons, houses, papers, and effects is triggered just as surely as if the government had entered our home and physically sorted through our financial, medical, familial, and associational records. Such queries therefore demand the same label as such a home invasion: search.