University of Maryland Francis King Carey School of Law
DigitalCommons@UM Carey Law

Faculty Scholarship | Francis King Carey School of Law Faculty

2013

The Right to Quantitative Privacy

David C. Gray
University of Maryland Franics King Karey School of Law, dgray@law.umaryland.edu

Danielle Keats Citron
University of Maryland Francis King Carey School of Law, dcitron@law.umaryland.edu

Follow this and additional works at: https://digitalcommons.law.umaryland.edu/fac_pubs

 Part of the Fourth Amendment Commons, and the Privacy Law Commons

Digital Commons Citation
98 Minnesota Law Review 62 (2013).

This Article is brought to you for free and open access by the Francis King Carey School of Law Faculty at DigitalCommons@UM Carey Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of DigitalCommons@UM Carey Law. For more information, please contact smccarty@law.umaryland.edu.

Article

The Right to Quantitative Privacy

David Gray[†] **& Danielle Citron**[††]

† Professor of Law, University of Maryland Francis King Carey School of Law.

†† Lois K. Macht Research Professor & Professor of Law, University of Maryland Francis King Carey School of Law, Affiliate Scholar, Stanford Center on Internet and Society, Affiliate Fellow, Yale Information Society Project. The authors thank everyone who generously commented on this work during presentations at Yale's Information Society Project, the Annual Meeting of the ABA/AALS Criminal Law Section, the University of North Carolina, Northwestern, Yale's Conference on Locational Privacy and Biometrics, Law and Society, the Privacy Law Scholars Conference, and the Computers, Freedom, and Privacy Conference, and during conversations at the American Law Institute Meeting on Information Privacy Law and Harvard Law Review's Symposium on Informational Privacy. Particular thanks go to Ronald Allen, Julia Angwin, Jack Balkin, Kevin Bankston, Steve Bellovin, Marc Blitz, Richard Boldt, Becky Bolin, Mary Bowman, Al Brophy, Andrew Chin, Bryan Choi, Thomas Clancy, Julie Cohen, Thomas Crocker, Nick Doty, LisaMarie Freitas, Susan Freiwald, Barry Friedman, Brandon Garrett, Bob Gellman, Don Gifford, Mark Graber, John Grant, James Grimmelmann, Deborah Hellman, Leslie Meltzer Henry, Lance Hoffman, Renée Hutchins, Camilla Hrdy, Orin Kerr, Joseph Kennedy, Catherine Kim, Anne Klinefelter, Avner Levin, Michael Mannheimer, Dan Markel, Christina Mulligan, Richard Myers, Neil Richards, Catherine Sabbeth, Laurent Sacharoff, Paul Schwartz, Christopher Slobogin, Robert Smith, Dan Solove, Max Stearns, David Super, Harry Surden, Peter Swire, Peter Quint, Jason Weinstein, Arthur Weisburd, and Jonathan Witmer-Rich. We also thank Liz Clark Rinehart for her research assistance and Max Siegel for his insightful editing. Finally, we are grateful to Frank Lancaster for holding us together. Copyright © by David Gray and Danielle Citron.

INTRODUCTION

In June and July 2013, documents leaked by a government contractor revealed details of three expansive surveillance programs operated by the Federal Bureau of Investigation (FBI) and the Department of Defense on behalf of the National Security Agency (NSA).[1] The first requires that Verizon and other telecommunication companies provide to the NSA on a daily basis "all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local

1. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [hereinafter Greenwald, *Phone Records*]; Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'* GUARDIAN, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [hereinafter Greenwald, *XKeyscore*].

telephone calls."[2] Although this program does not allow for the collection of content, including customers' conversations, telephony metadata is a rich source of information, giving authorities vast knowledge about callers' identity, location, and social networks.[3] A second program, referred to in leaked documents as "PRISM," reportedly allows the NSA and the FBI to access "audio and video chats, photographs, e-mails, documents, and connection logs" collected by nine leading U.S. internet companies, including Google and Facebook.[4] The third program, called XKeyscore, provides analysts with the capacity to mine content and metadata generated by e-mail, chat, and browsing activities through a global network of servers and internet access points.[5] These revelations confirm previous reports about a comprehensive domestic surveillance program that seeks to provide government agents with contemporary and perpetual access to details about everywhere we go and everything we do, say, or write, particularly when using or in the company of networked technologies.[6]

2. *Verizon Forced to Hand Over Telephone Data–Full Court Ruling,* GUARDIAN, June 5, 2013, http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order [hereinafter FISA]. The NSA subsequently released a declassified version of the order. *See Declassified Government Documents Related to NSA Collection of Telephone Metadata Records*, WASH. POST, http://apps.washingtonpost.com/g/page/politics/government-documents-related-to-nsa-collection-of-telephone-metadata-records/351/ (last visited Oct. 15, 2013).

3. Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelations*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records ("[Telephony] metadata . . . can provide authorities with vast knowledge about a caller's identity. . . . [C]ross-checked against other public records, the metadata can reveal someone's name, address, driver's license, credit history, social security number and more.").

4. Gellman & Poitras, *supra* note 1. The companies identified as participants in PRISM have denied granting government agents open access to their servers. *Id.* As of this writing, the full truth of the program remains hidden behind a veil of alleged national security necessity.

5. Greenwald, *XKeyscore*, *supra* note 1.

6. *See* JAMES BAMFORD, THE SHADOW FACTORY 177–96 (2008) [hereinafter BAMFORD, SHADDOW]; James Bamford, *The NSA Is Building the Country's Biggest Spy Center*, WIRED MAG., Mar. 15, 2012, *available at* http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1 [hereinafter Bamford, *The NSA is Building*]; Michael Isikoff, *The Fed Who Blew the Whistle*, NEWSWEEK (Dec. 12, 2008), http://www.thedailybeast.com/newsweek/2008/12/12/the-fed-who-blew-the-whistle.html; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 15, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

The domestic surveillance infrastructure is not confined to our networked communications, however. Consider aerial drones. No longer just a feature of modern warfare, unmanned aerial drones now populate domestic airspace.[7] Military-style drones operate along the United States border with Mexico.[8] Farther inland, law enforcement agencies are starting to use a variety of drones during their routine police operations.[9] Many of these drones are hardly visible, and some are as small as insects.[10] Among the primary advantages of these drone surveillance systems is that they are "covert."[11] As one operator reported: "You don't hear it, and unless you know what you're looking for, you can't see it."[12] Drones are also increasingly inexpensive, with some costing just a few hundred dollars.[13] Given the diversity, power, secrecy, and increasingly modest cost of aerial drones, we should expect them to become a more and more common presence in our skies.[14]

We are also increasingly subject to surveillance by systems capable of aggregating and analyzing large quantities of information from a variety of sources. Take, for example, New York's "Domain Awareness System" (DAS), which was unveiled by Mayor Michael Bloomberg and Police Commissioner Ray-

7. *See* Lev Grossman, *Drone Home*, TIME MAG., Feb. 11, 2013, at 28, 31–33; Jennifer Lynch, *Are Drones Watching You?*, ELECTRONIC FRONTIER FOUND. (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you. In the United States, "50 companies, universities, and government organizations are developing and producing some 155 unmanned aircraft designs." *Id.* In 2010, expenditures on unmanned aircraft in the United States exceeded three billion dollars and are expected to surpass seven billion dollars over the next ten years. *Id.*

8. Grossman, *supra* note 7, at 31.

9. *Id.* at 28, 32.

10. *See id.* at 33; John W. Whitehead, *Roaches, Mosquitoes and Birds: The Coming Micro-Drone Revolution*, HUFFINGTON POST (Apr. 17, 2013, 12:48 PM), http://www.huffingtonpost.com/john-w-whitehead/micro-drones-b-3084965.html.

11. Peter Finn, *Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate*, WASH. POST, Jan. 23, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

12. *Id.*

13. *See* Grossman, *supra* note 7, at 28.

14. *See* Lynch, *supra* note 7 ("[S]ome have forecast that by the year 2018 there will be 'more than 15,000 [unmanned aircraft systems] in service in the U.S., with a total of almost 30,000 deployed worldwide.'"). The pizza chain Domino's is also taking to the air with a delivery drone. *See Pizza-Delivery Drones? Domino's Gives it a Shot* (NPR radio broadcast June 5, 2013).

mond Kelly in August 2012.[15] Developed in conjunction with Microsoft,[16] DAS aggregates and analyzes video streams from 3,000 public and private security cameras, images from license-plate readers and traffic cameras, and data from government and private databases.[17] DAS will ensure the surveillance of New Yorkers and the city as a whole, twenty-four hours a day, seven days a week.[18] Confronted with comparisons to George Orwell's "Big Brother," Bloomberg replied, "What you're seeing is what the private sector has used for a long time. If you walk around with a cell phone, the cell phone company knows where you are . . . . We're not your mom and pop's police department anymore."[19]

New Yorkers are not the only people being monitored by increasingly expansive and sophisticated surveillance systems. The NYPD and Microsoft will be co-marketing DAS for sale to other municipalities.[20] There are also competitors, such as Alabama's joint venture with Google dubbed "Virtual Alabama," which collects and mines information from sources as diverse as surveillance cameras in public schools, three-dimensional satellite and aerial imagery, geospatial analytics, sex offender registries, and hospital inventories.[21]

15. Chris Dolmetsch & Henry Goldman, *New York, Microsoft Unveil Joint Crime-Tracking System*, BLOOMBERG NEWS (Aug. 8, 2012, 6:19 PM), http://www.bloomberg.com/news/2012-08-08/new-york-microsoft-unveil-joint-crime-tracking-system.html.

16. *Id.* New York and Microsoft are now marketing the Domain Awareness System to states and municipalities under a profit sharing plan. *See* Paul Harris, *NYPD and Microsoft Launch Advanced Citywide Surveillance System*, GUARDIAN, Aug. 8, 2012, http://theguardian.com/world/2012/aug/08/nypd-microsoft-surveillance-system.

17. Dolmetsch & Goldman, *supra* note 15; *see also* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 2 (2008) (reporting on plans to "mount thousands of cameras throughout Lower Manhattan to monitor vehicles and individuals").

18. *Public Security Privacy Guidelines*, N.Y.C. POLICE DEPARTMENT (Apr. 2, 2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf.

19. *NYPD's 'Domain Awareness' Surveillance System, Built by Microsoft, Unveiled by Bloomberg,* HUFFINGTON POST (Aug. 9, 2012, 12:51 PM), http://www.huffingtonpost.com/2012/08/09/nypd-domain-awareness-surveillance-system-built-microsoft_n_1759976.html?.

20. *Id.*

21. Corey McKenna, *Virtual Alabama Facilitates Data Sharing Among State and Local Agencies*, DIGITAL CMTYS. (Aug. 13, 2009), http://www.digitalcommunities.com/articles/Virtual-Alabama-Facilitates-Data-Sharing-Among.html.

Regional efforts like DAS and Virtual Alabama supplement a nationwide network of "fusion centers,"[22] which are operated as joint ventures between governmental agencies and private stakeholders to monitor, store, and mine the contents of electronic communications, public and private sector databases, health records, video feeds, and histories of online activity.[23] Along with these government-run ventures, the marketplace is increasingly populated by for-profit data aggregation companies like ChoicePoint and Acxiom that gather, analyze, package, and sell vast quantities of personal information on hundreds of millions of Americans for public and private clients.[24]

These discrete surveillance technologies and mass data collection efforts offer law enforcement and other government entities powerful tools in their ongoing efforts to prevent, detect, and prosecute crime, monitor border traffic, and guard against threats from international and domestic terrorists.[25] On the other hand, they implicate individual and collective expectations of privacy.[26] These competing interests raise important questions about the Fourth Amendment status of new and developing surveillance technologies. Should we leave the use of these technologies to the unfettered discretion of police officers? Or should we treat their use as "searches" subject to Fourth Amendment regulation, perhaps including the warrant requirement?

Similar questions came before the Court last year in *United States v. Jones*.[27] In that case, law enforcement officers used a GPS-enabled tracking device to monitor Jones's movements for four weeks, gathering over 2,000 pages of data in the pro-

22. Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1443 (2011).

23. *Id.* at 1451; DEP'T OF JUSTICE, HEALTH SECURITY: PUBLIC HEALTH AND MEDICAL INTEGRATION FOR FUSION CENTERS 8 (2011), *available at* www.it.ojp.gov/docdownloader.aspx?ddid=1450.

24. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595–96 (2004); Natasha Singer, *A Data Giant Is Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 17, 2012, at BU1.

25. See David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745 (2013), for our exploration of some of these interests.

26. *See infra* Parts I–II (discussing the potential problems with indiscriminate surveillance and how to handle it under the Fourth Amendment).

27. United States v. Jones, 132 S. Ct. 945, 954 (2012).

cess.[28] Although *Jones* was resolved on narrow grounds, concurring opinions indicate that at least five justices have serious Fourth Amendment concerns about law enforcement's growing surveillance capabilities.[29] Those justices insisted that citizens[30] possess a Fourth Amendment right to expect that certain quantities of information about them will remain private, even if they have no such expectations with respect to any of the discrete particulars of that information.[31] Thus, even if the use of a GPS-enabled tracking device to effect "relatively short-term monitoring of a person's movements on public streets" does not implicate the Fourth Amendment, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[32]

According to critics and supporters alike, this quantitative account of Fourth Amendment privacy is revolutionary.[33] In his majority opinion in *Jones*, Justice Scalia describes some of the challenges and dangers.[34] Foremost among these is the burden of explaining quantitative privacy's Fourth Amendment pedigree.[35] A quantitative approach to the Fourth Amendment appears to undercut well-established rules, including the public observation doctrine and the third-party doctrine.[36] Defenders of quantitative privacy must chart a conceptual link to these precedents or provide compelling reasons for changing course.[37] Advocates also must provide a workable test that law enforcement and courts can employ in drawing the line between quantities of data that do and do not trigger the Fourth Amend-

28. *Id.* at 948–49.

29. *See id.* at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

30. We use "citizen" here and throughout this article in a generic, nontechnical sense, to refer to all persons who can assert Fourth Amendment rights and protections.

31. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring) ("In the pre-computer 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 . . . . Devices like the [GPS-enabled tracking technology] used in the present case, however, make long-term monitoring relatively easy and cheap.").

32. *Id.* at 964.

33. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314–15 (2012).

34. *Jones*, 132 S. Ct. at 953–54.

35. *Id.* at 954. We answer this call in Part II.

36. *See infra* Parts IV.B, IV.D (analyzing the technology-centered approach alongside the public observation doctrine and the third-party doctrine).

37. We answer this demand in Part IV.

ment.[38] This Article responds to these demands by engaging the Information Privacy Law Project.[39]

Although information privacy law and Fourth Amendment jurisprudence have a shared interest in defining and protecting privacy, with the exception of a few information privacy scholars, these two fields have largely been treated as theoretically and practically discrete.[40] It is time to end that isolation and the mutual exceptionalism it implies. For nearly fifty years, scholars, activists, and policymakers working on information privacy law have warned about the dangers of surveillance technologies, including their capacity to chill projects of ethical self-development that are both core to our liberty interests and essential to a functioning democracy.[41] As we argue here, these concerns have clear Fourth Amendment salience and provide critical guidance as courts and legislatures search for ways to regulate emerging surveillance technologies in the shadow of *Jones*.

As a protection afforded to "the people," the Fourth Amendment erects a crucial constitutional bulwark against law enforcement's tendency to engage in broader and ever more intrusive surveillance when officers and agencies are left to their own discretion.[42] As Justice Jackson pointed out in *Johnson v. United States*,[43] law enforcement is a competitive enterprise in

38. *Jones*, 132 S. Ct. at 954. We describe and defend such a test *infra* Parts II and III.

39. Neil Richards coined this phrase to refer to the "collective effort by a group of scholars to identify a law of 'information privacy' and to establish information privacy law as a valid field of scholarly inquiry." Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006) (book review); *see also* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 197 (1995) (discussing information privacy policy entrepreneurs).

40. *See, e.g.*, DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011); Julie E. Cohen, *Privacy, Visibility, Transpareucy, and Exposure*, 75 U. CHI. L. REV. 181 (2008); Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

41. *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 3–4 (2007), *available at* http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1610–16 (1999).

42. *See* Balkin, *supra* note 17, at 1, 19 (exploring the "enormous political pressure" on law enforcement to use advanced surveillance and data mining technologies); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 556 (1999) ("[T]he larger purpose for which the Framers adopted the [Fourth Amendment was] to curb the exercise of discretionary authority by officers.").

43. Johnson v. United States, 333 U.S. 10 (1948).

which government agents will seek any strategic advantage available to them.[44] Pursuit of that advantage impels government agents, even those acting with the best of intentions, toward broader and more intrusive forms of surveillance.[45] Our eighteenth-century forebears knew well the dangers of leaving these natural motivations unchecked.[46] Before America's founding, British agents routinely abused general warrants, including writs of assistance, to subject our forefathers to the eighteenth-century equivalent of a surveillance state.[47] The Fourth Amendment responded to these abuses by limiting the right of law enforcement to effect physical searches and seizures and the authority of politically driven legislatures and executives to license programs of broad and indiscriminate search.[48]

Granting law enforcement unfettered access to twenty-first century surveillance technologies like aerial drones, DAS, and sweeping data collection efforts, implicates these same Fourth Amendment interests.[49] This does not mean that law enforcement should be barred from conducting searches using modern surveillance technologies. Instead, in the present, as in the past,[50] all that the Fourth Amendment requires is a set of policies and practices that limit the discretion of law enforcement, provide for meaningful judicial review, and effect a reasonable accommodation of both the legitimate interests of law enforcement in preventing, detecting, and prosecuting crime, and the privacy interests of citizens subject to surveillance.[51] Here

44. *Id.* at 14.

45. *Id.*

46. *See* United States v. Di Re, 332 U.S. 581, 595 (1948) ("But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment.").

47. *See infra* Part II.C.

48. *See* Davies, *supra* note 42, at 655–60, 668.

49. *Infra* Parts III.B–D (discussing the Fourth Amendment implications of these technologies).

50. *See generally* Davies, *supra* note 42, at 578–80 ("Common-law authorities repeatedly gave a consistent reason for condemning general warrants: if such warrants had been permitted, they would have conferred on ordinary officers *discretionary authority* to arrest or even to search houses. . . . Hostility to conferring discretionary search authority on common officers is also the theme of American complaints about the general writ of assistance.").

51. *See, e.g.*, United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

again, the work of information privacy law scholars offers important guidance in striking that balance.[52]

Until now, most proposals for defending Fourth Amendment interests in quantitative privacy have focused on a case-by-case method called the "mosaic theory."[53] Under this approach, the Fourth Amendment is implicated whenever law enforcement officers gather "too much" information during the course of a specific investigation.[54] Critics of the mosaic theory have rightly wondered how courts will determine whether investigators have gathered too much information in any given case and how officers in the midst of ongoing investigations will know whether the aggregate fruits of their efforts are approaching a Fourth Amendment boundary.[55] The best solution that mosaic advocates have so far been able to muster is to draw bright, if arbitrary, lines based on how long officers use an investigative method or technology.[56] These kinds of solutions fail to satisfy because they are under inclusive, over inclusive, and also sidestep important conceptual and doctrinal questions.[57] We therefore propose an alternative.

Rather than asking *how much* information is gathered in a particular case, we argue here that Fourth Amendment interests in quantitative privacy demand that we focus on *how* information is gathered. In our view, the threshold Fourth Amendment question should be whether a technology has the

52. *See supra* note 39.

53. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 556–58 (2010) (asserting that the *Knotts* analysis is limited to the specific facts of the case); Kerr, *supra* note 33, at 311; Richard McAdams, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 340 (1985); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CON. L. & PUB. POL'Y (forthcoming 2012) (manuscript at 1), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2098002. See David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (2013), for our discussion of conceptual, doctrinal, and practical questions raised by the mosaic theory.

54. *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring); *Maynard*, 615 F.3d at 562; Gray & Citron, *supra* note 53, at 390.

55. *See, e.g.*, *Jones*, 132 S. Ct. at 953–54; Gray & Citron, *supra* note 53, at 408–11; Kerr, *supra* note 33, at 328–30.

56. *See, e.g.*, *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring); Slobogin, *supra* note 53 (manuscript at 3, 28).

57. *See* Gray & Citron, *supra* note 53, at 426–28. Professor Slobogin acknowledges this concern, but nevertheless favors a regulatory scheme based on duration of surveillance for purposes of administrability. *See* Slobogin, *supra* note 53 (manuscript at 28).

capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents.[58] If it does not, then the Fourth Amendment imposes no limitations on law enforcement's use of that technology, regardless of how much information officers gather against a particular target in a particular case.[59] By contrast, if it does threaten reasonable expectations of quantitative privacy, then the government's use of that technology amounts to a "search," and must be subjected to the crucible of Fourth Amendment reasonableness, including judicially enforced constraints on law enforcement's discretion.[60]

The form and timing of Fourth Amendment constraint under our proposal would depend upon the technology at issue, the law enforcement interests it serves, and the privacy interests it threatens.[61] The most common way to implement Fourth Amendment regulations is to require officers to secure warrants from a detached and neutral magistrate before engaging in a search.[62] For some technologies, that model will remain the best approach; but it is not the only alternative. Although ultimate authority to review constitutional sufficiency must remain with the judiciary as a constitutional matter,[63] our technology-centered approach allows for a range of more bespoke arrangements. For example, Congress might create a tailored regime along the lines of the Title III Wiretap Act.[64] Alterna-

58. In proposing a technology-based approach to quantitative privacy, we are inspired by the work of Susan Freiwald. *See, e.g.*, Freiwald, *supra* note 41, ¶ 9 (offering a technology-based approach to regulating government interference with electronic communications).

59. The political branches would of course be free to impose extra-constitutional limitations on the use of these investigative technologies. *See infra* Part III.B–C. That the Fourth Amendment is silent would not at all prejudice the authority of the political branches to impose extra-constitutional limitations on the use of investigative technologies that do not implicate quantitative privacy. As we point out below, Congress has taken steps in the past to regulate the use of wiretaps and pen register devices after the Court declined to impose Fourth Amendment limitations on the use of these technologies. *See infra* notes 456–58 and accompanying text.

60. *See Jones*, 132 S. Ct. at 948, 950.

61. *See infra* Part III.

62. *See* Peter P. Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 915–16 (2004).

63. Balkin, *supra* note 17, at 23.

64. *See* Swire, *supra* note 62, at 923, 930.

tively, a law enforcement agency might collaborate with civil liberties groups and other interested parties to develop regulations and administrative control structures[65] similar to the consent decrees that are often used to resolve constitutional challenges against police surveillance tactics and practices.[66] As part of these efforts, designers and developers of surveillance technologies might incorporate constraints on the aggregation and retention of data along with use and access limitations, providing a set of Fourth Amendment pre-commitments that preserve law enforcement interests while minimizing threats to privacy.[67]

In what follows, we make the case for the right to quantitative privacy and a technology-centered approach to protecting that right. Part I draws from the Information Privacy Law Project to explain the threats to personality development, democratic participation, and accurate judgments posed by technologies capable of facilitating broad programs of indiscriminate surveillance. Part II explains the Fourth Amendment relevance of these concerns. Part III offers concrete proposals for protecting Fourth Amendment interests in quantitative privacy by considering how our technology-centered approach would apply to different kinds of surveillance technology. Part IV responds to objections and challenges.

I. QUANTITATIVE PRIVACY: THE PERILS OF BROAD AND INDISCRIMINATE SURVEILLANCE

Although concerns about technology's expanding capacities to gather and aggregate large quantities of data are new to Fourth Amendment jurisprudence, they have for decades been the focus of the Information Privacy Law Project, a longstanding effort by scholars, practitioners, and activists to understand privacy, its importance to individuals and society, and law's role in protecting it.[68] As early as the 1960s, contributors to this project began raising concerns about the privacy implications of then-nascent computer databases.[69] Public and pri-

65. *See, e.g.*, Balkin, *supra* note 17, at 24 (suggesting that Congress can create a group in the Executive branch made up of independent privacy experts).

66. *See*, *e.g.*, Handschu v. Special Servs. Div., 605 F. Supp. 1384, 1389–92, 1417 (S.D.N.Y. 1985).

67. *See infra* Part III.C.

68. *See* sources cited *supra* note 39.

69. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 158–63 (1967) (discussing the "current pressures on privacy").

vate entities had begun amassing computerized dossiers of people's activities that armies of investigators could never have accumulated on their own.[70] Businesses digitized employment, customer, and medical records; governments generated digital records on millions of Americans, including "subversives," Social Security participants, and public benefits recipients; and direct-mail companies categorized consumers and sold their personal information.[71]

Widespread public anxiety soon emerged about these "Big Brother" computer databases.[72] From 1965 through 1974, nearly fifty congressional hearings and reports investigated a range of data privacy issues, including the use of census records, access to criminal history records, employers' use of lie detector tests, and monitoring of political dissidents by the military and law enforcement.[73] State and federal executives spearheaded investigations of surveillance technologies including a proposed National Databank Center.[74] Popular culture and public discourse was consumed with the "data-bank problem."[75]

This was not lost on the courts. In *Whalen v. Roe*,[76] a 1977 case involving New York's mandatory collection of prescription drug records, the Supreme Court strongly suggested that the Constitution contains a right to information privacy based on substantive due process.[77] Although it held that New York's prescription drug database did not violate the constitutional right to privacy because the gathered information was adequately secured, the Court recognized an "individual interest in avoiding disclosure of personal matters."[78] Writing for the Court, Justice Stevens noted the "threat to privacy implicit in the accumulation of vast amounts of personal information in

70. *Id.*

71. *See generally* NAT'L ACAD. OF SCIS., DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY (1972) (detailing data practices of several organizations). Columbia University Professor of Public Law Alan Westin, serving as Director of the National Academy of Science's Computer Science and Engineering Board, helped lead the study of governmental, commercial, and private organizations using computers to amass dossiers on individuals, featuring fourteen case studies after visiting and interviewing fifty-five organizations. *Id.* at 5.

72. *See* REGAN, *supra* note 39, at 13–15.

73. *Id.* at 7; NAT'L ACAD. OF SCIS., *supra* note 71, at 4–5.

74. NAT'L ACAD. OF SCIS., *supra* note 71, at 4–5.

75. *See id.*; REGAN, *supra* note 39, at 13.

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

77. *Id.* at 589, 598–600.

78. *Id.* at 599–600.

computerized data banks or other massive government files."[79] In a concurring opinion, Justice Brennan warned that the "central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[80]

This century's surveillance technologies pose far greater threats to privacy than the "Big Brother databanks" of the twentieth century. Information gathering is faster, cheaper, and more comprehensive than ever before.[81] Whereas information gathered by public and private entities once tended to remain in information silos, it is now seamlessly shared with countless organizations via the Internet.[82] Aggregation technology and advanced statistical analysis tools have enhanced the capacities of those who wield surveillance technology to know us, often in ways that we do not know ourselves.[83] Cheap data storage has virtually eliminated the privacy protections previously afforded by the possibility that past mistakes might be forgotten.[84] Data broker databases, for instance, contain thousands of data points about millions of individuals.[85]

Over the past fifty years, the Information Privacy Law Project has highlighted the dangers posed by these "dataveillance" technologies and their ability to systematically amass information about our daily lives.[86] Scholars have paid particular at-

79. *Id.* at 605.

80. *Id.* at 606 (Brennan, J., concurring).

81. Citron & Pasquale, *supra* note 22, at 1459.

82. *Id.*

83. Balkin, *supra* note 17, at 12; TECH. & PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM, 36–37 (2004) [hereinafter TAPAC].

84. Balkin, *supra* note 17, at 13–15.

85. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 246–48 (2007). Data brokers maintain websites custom-tailored for law enforcement that provide access to massive digital dossiers. As an internal document from the United States Marshals Service notes, "With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes" including Social Security numbers, known addresses, vehicle information, telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapon permits, liens, lawsuits, marriage licenses, and the like. Hoofnagle, *supra* note 24, at 596. Data brokers now combine that information with social media activity scrapped online, store purchases, and online surfing habits culled from online advertisers.

86. DAVID LYON, THE ELECTRONIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 57–80 (1994). Roger Clarke offered the term "dataveillance" as a way

tention to the damaging effects of surveillance on life projects central to personal liberty, including individuals' ethical exploration, identity development, self-expression, and self-actualization.[87] As they have shown, government surveillance (or its possibility) causes people to internalize the notion of being watched, even if it is not actually happening,[88] because "[*p*]*otential* knowledge can equal *present* power."[89] Government surveillance constrains "the acceptable spectrum of belief and behavior," resulting in a "subtle yet fundamental shift in the content of our character."[90] People move towards the benign and mainstream, which threatens "not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[91] In the face of broad and in-

to conceptualize new forms of surveillance facilitated by the widespread use of computer-based technology. Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 499, 502–04 (1988). Clarke identified two forms of dataveillance: (1) personal dataveillance, which involves identifiable persons who by their actions have attracted the attention of the panoptic system, and (2) mass dataveillance, which refers to gathering of data about groups of people with the intention of finding individuals requiring attention.

87. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 108 (2008) [hereinafter SOLOVE, UNDERSTANDING]; Cohen, *supra* note 40, at 194–97; TAPAC, *supra* note 83, at 35 ("Awareness that the government may, without probable cause or other specific authorization, obtain access to myriad, distributed stores of information about an individual may alter his or her behavior. People are likely to act differently if they know their conduct *could be* observed."); *see* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 44–47 (2004) (discussing the causes of self-censoring) [hereinafter SOLOVE, DIGITAL PERSON]. Studies have shown that people experience anxiety about being watched and misunderstood. Stuart A. Karabenick & John R. Knapp, *Effects of Computer Privacy on Help-Seeking*, 18 J. APPLIED SOC. PSYCHOL. 461 (1988).

88. SOLOVE, UNDERSTANDING, *supra* note 87, at 109; Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 403–04 (2008). *See also* GEORGE ORWELL, 1984 at 4 (1949) ("There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinised.").

89. TAPAC, *supra* note 83, at 35.

90. Julie E. Cohen, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE 141 (2012); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425–26 (2000) [hereinafter Cohen, *Examined*].

91. Cohen, *Examined, supra* note 90, at 1426. *See also* Hubert H. Humphrey*, Foreword to* EDWARD V. LONG, THE INTRUDERS, at viii (1967) ("We act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and

discriminate data collection about their daily activities, individuals cannot make meaningful choices about their activities, preferences, and relations and act on them without fear of embarrassment or recrimination.[92] Individual development and expression are inevitably chilled.[93]

The Information Privacy Project has also warned about the stakes of broad and indiscriminate surveillance for a healthy democracy.[94] Privacy preserves space for engaging in the critical functions of citizenship.[95] Self-rule requires a "group-oriented process of critical discourse" among autonomous individuals.[96] The persistent logging of our online activities and of-

our very character will change."); TAPAC, *supra* note 83, at 35–36 ("The greatest risk of government data mining is that access to individually identifiable data chills individual behavior . . . changing the legal behavior of U.S. persons, encouraging conformance with a perceived norm, discouraging political dissent, or otherwise altering participation in political life.").

92. ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 17 (2011); *see* Gary T. Marx, *Identity and Anonymity: Some Conceptual Distinctions and Issues for Research*, *in* DOCUMENTING INDIVIDUAL IDENTITY 311, 316, 318 (Jane Caplan & John Torpey eds., 2001) (discussing the benefits of anonymity). Aside from the consequential effects of surveillance technologies, privacy scholars also emphasize deontological concerns, notably that surveillance technologies demonstrates a lack of respect for its subject as an autonomous person. Stanley Benn explains that being "an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes." Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XIII: PRIVACY 1, 7 (J. Roland Pennock & John W. Chapman eds., 1971). The observed person sees herself as a knowable object, with "limited possibilities rather than infinite, indeterminate possibilities." *Id.* Covert surveillance is problematic because it "deliberately deceives a person about his world, thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice." *Id.* at 10.

93. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143–44 (2007); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 253–55 (2002). As Justice William O. Douglas observed, "[m]onitoring, if prevalent, certainly kills free discourse and spontaneous utterances." United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting).

94. *See, e.g.*, Balkin, *supra* note 17, at 17–18.

95. *See, e.g.*, STEPHEN BREYER, ACTIVE LIBERTY 3–5, 15–17, 66–74 (2005); MICHAEL J. SANDEL, DEMOCRACY'S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY 350 (1996) (discussing a democratic role for privately negotiated identities); Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 51–52 (2009).

96. Paul M. Schwartz, *Privacy and Participation: Personal Information and the Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560–61 (1995); *see also* TAPAC, *supra* note 83, at 35–36. Paul Schwartz has relied on the work of constitutional theorist James E. Fleming in arguing that democracy in general and constitutional law in particular must secure the

fline travels interferes with civic participation and deliberation.[97] As Spiros Simitis cautions, "neither freedom of speech nor freedom of association nor freedom of assembly can be fully exercised as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed."[98] For these reasons, privacy advocates have pressed for laws that can prevent "state or community intimidation that would destroy their involvement in the democratic life of the community."[99] In their view, "privacy in public" is indispensable for a functioning democratic society.[100]

preconditions for "'citizens to apply their capacity for a conception of the good to deliberat[ions] about . . . how to live their own lives.'" Schwartz, *supra* note 41, at 1654 (quoting James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 2–3 (1995)). Fleming calls for a deliberative autonomy that is based on moral autonomy, responsibility, and independence. James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 30–34 (1995).

97. Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822 (2010). What's more, a troubling power imbalance emerges between individuals and the entities that amass their information. Neil Richards, *The Dangers of Surveillance*, HARV. L. REV. (forthcoming 2013) (manuscript at 28), *available at* http://www.harvardlawreview.org/symposium/papers2012/richards.pdf. Individuals become vulnerable to the whims of powerful entities. SOLOVE, DIGITAL PERSON, *supra* note 87, at 44–47. During the 1950s and 1960s, civil rights, antiwar, and communist activists included on the FBI's "suspicious persons list" lost jobs, work opportunities, and licenses, while labor union organizers assumed new names and Social Security numbers due to fierce hostility to union members. NAT'L ACAD. OF SCIS., *supra* note 71, at 40, 41 (noting that in 1972 the Social Security Agency (SSA) permitted individuals to assume different identities and new Social Security numbers so that they could avoid prejudice due to their group affiliations); *see, e.g.*, Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA Patriot Act in the Context of Cointelpro and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1080–98 (2002) (detailing and criticizing the FBI's COINTELPRO domestic surveillance program of the 1950s, 1960s, and 1970s).

98. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987); *see also* TAPAC, *supra* note 83, at 34 (explaining that "awareness that the government may, without individual consent or judicial authorization, obtain access to myriad, distributed stores of information about an individual may have a chilling effect on commercial, social, and political activity. Informational privacy is, therefore, linked to other civil liberties, including freedom of expression, association, and religion").

99. Schwartz, *supra* note 96, at 561. This is not to suggest that the surveillance of groups is justiciable, although it may be in circumstances where the chilling of expressive association is accompanied by objective harm, such as reputational damage. *See* Laird v. Tatum, 408 U.S. 1, 13–14 (1972) (refusing to find justiciable constitutional violation for army's data gathering about political group because allegations of "subjective 'chill'" based on possibility that army may "at some future date misuse the information" are "not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm"); *see also* Linda E. Fisher, *Guilt by Expressive Associa-*

This is not to say that citizens subjected to invasive surveillance inevitably withdraw from democratic engagement. They may engage in productive resistance[101] or disregard surveillance's risks on the view that they have nothing to hide.[102] Nonetheless, the impulse to self-censor is strong when people have no idea who is watching them and how their information will be used.[103] This is all the more true for traditionally subordinated groups in our post-9/11 age.[104] Because racial, ethnic, and religious minorities are particularly vulnerable to governmental suspicion and profiling, they are more likely to refrain from both exploring their own conceptions of the good life and participating robustly in public life when they are subjected to surveillance.[105] The burden of self-censorship occasioned by a surveillance state is thus borne unequally. At any rate, democratic participation just should not require heroic levels of civic courage—such a requirement is both contrary to our constitu-

tion: Political Profiling, Surveillance, and the Privacy of Groups, 46 ARIZ. L. REV. 621, 656–57 (2004).

100. *See, e.g.*, Balkin, *supra* note 17, at 18; TAPAC, *supra* note 83, at 36 ("For two hundred years Americans have proudly distrusted their government. The risk, therefore, of the power to access data from disparate sources is not merely to informational privacy, but to civil liberties including freedom of expression, association, and religion.").

101. Kevin D. Haggerty, *Tear Down the Walls: On Demolishing the Panopticon*, *in* THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND 23, 34–35 (David Lyon ed., 2006).

102. SOLOVE, *supra* note 40, at 1.

103. As Frank Pembleton, portrayed by Andre Braugher in the NBC serial *Homicide: Life on the Street*, put the point: "[I]f you feel like you're being watched, you do what you're told, especially when you're being watched by someone you can't see." *Homicide: Life on the Street: Fits Like a Glove* (NBC television broadcast Oct. 21, 1994).

104. For example, in *Holder v. Humanitarian Law Project*, the Supreme Court upheld a content-based restriction of speech for offering material support to state-identified terrorist organizations, even if the money was given for humanitarian efforts. 130 S. Ct. 2705, 2729–31 (2010).

105. *See, e.g.*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 760–64 (2008) (noting that relational surveillance can "chill tentative associations and experimentation with various group identities); *see also* FREDERICK SCHAUER, PROFILES, PROBABILITIES, AND STEREOTYPES 22, 134–54, 158–60, 219 (2003) (exploring the problematic nature of predictive models when cued by race and gender because they are overused as markers of difference in morally problematic ways). One might argue that private entities also have the capacity to suppress by surveillance. We address these concerns *infra* Part IV.C–D.

tional scheme[106] and an undue burden on citizens of a free and democratic society.[107]

Courts operating in the information privacy context have echoed concerns that broad and indiscriminate surveillance threatens liberty interests.[108] For instance, in *Nader v. General Motors Corp.*,[109] General Motors undertook a campaign to discredit and intimidate its well-recognized critic Ralph Nader. The company placed him under extensive public surveillance and tapped his telephone.[110] In 1970, the New York Court of Appeals recognized that, although observing others in public places generally does not constitute a tort, sometimes "surveillance may be so 'overzealous' as to render it actionable."[111] As the court explained, "[a] person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing."[112]

The Information Privacy Law Project has also highlighted problems caused by incorrect or incomplete information amassed in databases.[113] In an early case confronting these issues, United States District Judge Gerhard Gesell ordered the FBI to refrain from disseminating computerized criminal records for state and local employment and license checks, because the records were often inaccurate and hence "clearly invade[d] individual privacy."[114] The court warned of ever more inaccuracies in databases with the "development of centralized state information centers to be linked by computer to the Bureau."[115]

Experience has shown that Judge Gesell's concerns were well founded. In recent years, employers have refused to interview or hire individuals based on incorrect or misleading per-

106. TAPAC, *supra* note 83, at 36.

107. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 837 (2000).

108. *See, e.g.*, Sanders v. Am. Broad. Co., 978 P.2d 67, 73–77 (Cal. 1999) (finding that a television show invaded an employee's privacy by secretly videotaping his workplace conversations even though other employees could hear him because employee should not reasonably expect to be secretly recorded by journalists).

109. 255 N.E. 2d 765, 767 (N.Y. 1970).

110. *Id.*

111. *Id.* at 771.

112. *Id.*

113. *See* TAPAC, *supra* note 83, at 37–39.

114. United States v. Menard, 328 F. Supp. 718, 726 (D.C. Cir. 1971).

115. *Id.* at 727.

sonal information obtained through surveillance technologies.[116] Governmental data-mining systems have flagged innocent individuals as persons of interest, leading to their erroneous classifications as terrorists or security threats, intense scrutiny at airports, denial of travel, false arrest, and loss of public benefits.[117] The potential for damage is magnified by our "information sharing environment," which facilitates the distribution of such designations with countless public and private actors, compounding the error in ways that are difficult to detect and eliminate.[118]

Consider the distortions generated by fusion centers that gather intelligence on "all hazards, all crimes, and all threats."[119] In one case, Maryland state police exploited their access to fusion centers to conduct surveillance of human rights groups, peace activists, and death penalty opponents over a nineteen-month period.[120] Fifty-three political activists eventually were classified as "terrorists," including two Catholic nuns and a Democratic candidate for local office.[121] The fusion center shared these erroneous terrorist classifications with federal drug enforcement, law enforcement databases, and the National Security Administration, all without affording the innocent targets any opportunity to know, much less correct, the record.[122]

116. SOLOVE, DIGITAL PERSON, *supra* note 87, at 46–47. Only in exceptional cases do individuals discover their digital dossiers contain erroneous information about them. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1816 n.82 (2010).

117. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1273–77 (2008) (exploring inaccuracies of automated decision-making governmental systems including "No Fly," public benefits, and "dead beat" parent matching systems).

118. Citron & Pasquale, *supra* note 22, at 1443 (describing data inaccuracy risks, including those linked to data integration attempts). Federal agencies, including the Department of Homeland Security, gather information in conjunction with state and local law enforcement officials in what Congress has deemed the "information sharing environment" (ISE). *Id.* The ISE is essentially a network; its hubs are fusion centers whose federal and state analysts collect, analyze, and share intelligence. *Id*; *see* TAPAC, *supra* note 83, at 37–39.

119. Citron & Pasquale, *supra* note 22, at 1450.

120. Nick Madigan, *Spying Uncovered*, BALT. SUN, July 18, 2008, at A1.

121. Citron & Pasquale, *supra* note 22, at 1462.

122. Madigan, *supra* note 120. The ACLU found out about the erroneous classifications by sheer luck. After activists shared their concerns about being watched at meetings, it filed open sunshine requests, which eventually yielded information about the monitoring and the fusion center's involvement. Once the press covered the story, the state Attorney General initiated an investigation of the matter, exposing detailed information about the abuse. Danielle

The dangers of powerful data aggregation and analysis technologies are not limited to mistakes, of course. If anything, the threats to liberty and democratic culture are more profound if they are accurate. On this point, Jack Balkin has argued that, "Government's most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data."[123] What is collected need not be particularly intimate or private, he continues; rather, "data mining technologies allow the state and business enterprises to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people's behavior, beliefs, and attitudes."[124] From this level of surveillance, he concludes, government dominance and control follows.[125]

Work done in the information privacy law context provides ample evidence that programs of broad and indiscriminate surveillance threaten fundamental liberty interests and democratic values. Despite the critical role played by privacy concepts in contemporary Fourth Amendment doctrine, however, there has been little interdisciplinary engagement between the Information Privacy Law Project and Fourth Amendment law and scholarship. The Court's decision in *United States v. Jones*[126] invites us to end that isolation. The next Part accepts that invitation.

Keats Citron, *COINTELPRO in a Digital World*, CONCURRING OPINIONS (Oct. 11, 2008, 3:00 PM), http://www.concurringopinions.com/archives/2008/10/cointelpro_in_a.html.

123. Balkin, *supra* note 17, at 12. This point draws on the work of Michel Foucault who extended Bentham's insights to describe how a whole range of public institutions use surveillance to shape subjects who internalize the norms and priorities of the institutions in which they are situated. MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–308 (1975); *see also* MICHEL FOUCAULT, MADNESS AND CIVILIZATION: A HISTORY OF INSANITY IN THE AGE OF REASON (1961).

124. Balkin, *supra* note 17, at 12. *See also* TAPAC, *supra* note 83, at 39–40 (describing how innocuous information, such as special meal requests made to an airline, can be misused by government surveillance programs to identify and target individuals based on religious affiliation).

125. Balkin, *supra* note 17, at 12–15.

126. 132 S. Ct. 945 (2012).

II. QUANTITATIVE PRIVACY AND THE FOURTH AMENDMENT

In a landmark near-decision, the Supreme Court almost held in *United States v. Jones*[127] that citizens have a Fourth Amendment interest in quantitative privacy. Although resolved on narrow grounds, five Justices raised concerns in *Jones* about the capacity of surveillance technologies to gather large quantities of data that reveal personal details about our lives.[128] In the wake of *Jones*, critics and skeptics of this quantitative account of Fourth Amendment privacy have leveled charges of doctrinal radicalism and impracticality.[129] In this Part and the next we draw on insights from the Information Privacy Law Project to meet these challenges. We begin with a brief history of Fourth Amendment doctrine to put *Jones* in context.

A. QUALITATIVE PRIVACY: THE FOURTH AMENDMENT BEFORE *UNITED STATES V. JONES*

Although not specified in the text,[130] for at least a century after the Fourth Amendment was ratified, courts defined "search" in reference to concepts of common law trespass.[131] As a consequence, Fourth Amendment rights were linked to property rights and Fourth Amendment remedies were limited to suits in tort.[132] That changed in the twentieth century with increased urbanization, emerging transportation and communication technologies, and the expansion of professionalized police forces.[133] *Olmstead v. United States*[134] marks the beginning of the shift.[135]

127. *Id.* at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

128. *Id.* at 954 (Sotomayor, J., concurring); *id*. at 957 (Alito, J., concurring).

129. Kerr, *supra* note 33, at 314–15, 346–52.

130. The Fourth Amendment provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

131. Slobogin, *supra* note 53, at 3–4. *But see* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, SUP. CT. REV. (forthcoming 2013) (manuscript at 2) (arguing that the trespass test of Fourth Amendment search is a myth created by the Court in *Katz* (citing Katz v. United States, 389 U.S. 347 (1967))), *available at* http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2169926_code810317.pdf?abstractid=2154611&mirid=1.

132. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786 (1994).

133. Olmstead v. United States, 277 U.S. 438, 471–79 (1928) (Brandeis, J.,

Writing for a five-justice majority in *Olmstead*, Chief Justice Taft held that intercepting telephone conversations was not a "search" under the Fourth Amendment because the technology used did not require any physical invasion of Olmstead's home.[136] In a spirited dissent, Justice Brandeis argued that this property-based approach to the Fourth Amendment was anachronistic.[137] As Justice Brandeis explained, it failed to protect citizens from procedures that might not require the "force and violence" necessary to invade property, but nevertheless compromised the sanctity of citizens' thoughts, beliefs, and emotions as well as the "individual security" they invested in activities like telephone conversations.[138]

Nearly four decades later, Justice Brandeis's view prevailed in *Katz v. United States*.[139] There, the Court held that using a listening device to monitor telephone conversations in a public phone booth constituted a Fourth Amendment "search" despite the absence of a physical intrusion.[140] In rejecting the trespass requirement, the Court famously declared that, "the Fourth Amendment protects people, not places."[141] The Court found that conversations in public telephone booths deserve Fourth Amendment protection because citizens expect that their telephone conversations are just as secure from public review as their daily domestic routines in the home.[142] Although phone booths are open to public view, the Court noted that they

dissenting); Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure, 1850–1940*, 62 RUTGERS L. REV. 447, 460–61 (2010); *see also* DAVID R. JOHNSON, POLICING THE URBAN UNDERWORLD 4–9, 29–40 (1979).

134. 277 U.S. 438 (1928).

135. Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 423–24 (2007).

136. *Olmstead*, 277 U.S. at 466.

137. *Id.* at 473–74 (Brandeis, J., dissenting). Justice Brandeis' dissent came as no surprise to students of his groundbreaking article, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), which he co-wrote with Samuel D. Warren.

138. *Olmstead*, 277 U.S. at 473–74, 478–79 (Brandeis, J., dissenting) ("[The Framers] recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men.").

139. 389 U.S. 347 (1967).

140. *Id.* at 353, 358–59.

141. *Id.* at 351.

142. *Id.* at 351–52.

function as spaces of aural repose.[143] Thus, citizens could reasonably expect that their communications in telephone booths would not be monitored by "uninvited ear[s]," even if they can be seen by "intruding eye[s]."[144] The other alternative—declining to extend Fourth Amendment protection at all—would unsettle these broadly held expectations and raise the specter of a surveillance state.[145]

After *Katz*, determining whether government conduct constitutes a Fourth Amendment "search" has turned on whether the person claiming a violation subjectively manifests an expectation of privacy that society is prepared to recognize as reasonable.[146] Of course, we enjoy a broader range of reasonable privacy expectations in some places than in others.[147] For example, we harbor strong expectations of privacy in our homes, persons, and immediate possessions.[148] By contrast, as the Court has ruled, we have no reason to expect privacy in activities we "knowingly expose[] to the public."[149] Between these endpoints, we have "diminished" expectations of privacy in our cars[150] and businesses[151] because our activities in these spaces are often, but not always, exposed to the public or to regulators. Under the *Katz* test, however, the key question in Fourth Amendment cases is not *where* a search occurs, but *whether* and *to what degree* it invades reasonable expectations of privacy.[152] This is the qualitative approach to the Fourth Amendment.

143. *Id.*

144. *Id.* at 352.

145. *Id.* at 354–59 (interposing a warrant requirement for electronic eavesdropping and emphasizing that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored 'the procedure of antecedent justification . . . that is central to the Fourth Amendment,' a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case").

146. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012).

147. Slobogin, *supra* note 53, at 5–7.

148. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (discussing the strong expectation of privacy in one's home); U.S. CONST. amend. IV (mentioning "persons, houses, papers, and effects" as being specifically protected from unwarranted searches and seizures).

149. Katz v. United States, 389 U.S. 347, 351 (1967).

150. Wyoming v. Houghton, 526 U.S. 295, 300, 304–05 (1999).

151. New York v. Burger, 482 U.S. 691, 700 (1987).

152. *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

Applying this qualitative approach, the Court has formulated two important legal doctrines that are implicated by *United States v. Jones*. First, establishing what is known as the "public observation doctrine," the Court has held that law enforcement officers can freely make observations from any place where they lawfully have a right to be.[153] Police officers thus may stand on the street and observe us through open windows, look down on us from public airspace,[154] and monitor our movements on public roads.[155] Officers may also use devices such as binoculars, telephoto lenses,[156] and beeper-type trackers[157] to enhance their observational abilities.

Second, the Court has held that the Fourth Amendment cannot save us from "misplaced confidence" in third parties.[158] Even if we avoid public exposure by only sharing our private activities with a select few, we run the risk that those people will violate our trust by sharing the details with law enforcement.[159] Applying this "third-party doctrine," the Court has held that the Fourth Amendment does not prohibit the government from lawfully obtaining privately recorded conversations that are disclosed by the recording party,[160] a list of numbers dialed from a customer's telephone that is obtained by the telephone company using a "pen register,"[161] or lists of financial transactions passed along by a customer's bank.[162] Part of the reason why critics dismiss the quantitative approach to privacy articulated in the *Jones* concurrences is because it appears to threaten both the public observation doctrine and the third party doctrine.[163]

153. Florida v. Riley, 488 U.S. 445, 449–50 (1989).

154. California v. Ciraolo, 476 U.S. 207, 215 (1986).

155. United States v. Knotts, 460 U.S. 276, 281–82 (1983).

156. Dow Chemical Co. v. United States, 476 U.S. 227, 251 (1986).

157. *Knotts*, 460 U.S. at 281–82.

158. United States v. White, 401 U.S. 745, 777 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966).

159. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (describing Supreme Court cases rejecting Fourth Amendment challenges to evidence gathered from undercover agents and confidential informants).

160. Lopez v. United States, 373 U.S. 427, 438–39 (1963); *see also* United States v. Davis, 326 F.3d 361, 366–67 (2d Cir. 2003).

161. Smith v. Maryland, 442 U.S. 735, 741–42 (1979).

162. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21 (1974). As Part IV discusses, Congress passed legislation to protect the privacy interests in the contents of bank records that are not reached by the Fourth Amendment.

163. *See infra* Part IV.B–D.

B. A FOURTH AMENDMENT FOOTHOLD FOR QUANTITATIVE PRIVACY IN *UNITED STATES V. JONES*

In *United States v. Jones*, an inter-agency group of law enforcement officers suspected that Jones was a high-level participant in a conspiracy to distribute narcotics in and around the District of Columbia.[164] Jones was cautious, however, which prevented officers from developing enough direct evidence to justify his arrest and prosecution.[165] Fortunately for them, officers had enough evidence to apply for warrants allowing them to "tap" his telephone and to monitor his movements with a GPS device attached to his Jeep.[166] These efforts produced several incriminating statements and over 2000 pages of tracking data showing that Jones made regular visits to stash houses and other locations tied to the broader drug conspiracy during the twenty-eight day monitoring period.[167] Unfortunately, the officers violated the terms of their tracking warrant when installing the GPS device, which left the door open for Jones to object to the introduction of this evidence at trial.[168]

Relying on the public observation doctrine, the trial court denied Jones's motion to suppress.[169] Jones subsequently was convicted, in part based upon the GPS data, which provided a critical link between him and the alleged drug conspiracy.[170] On appeal, the United States Court of Appeals for the District of Columbia Circuit reversed.[171] Writing for the panel, Judge Ginsburg argued that there is a Fourth Amendment distinction between short-term and long-term monitoring.[172] Although movements in public can be observed in discrete time slices by anyone—including law enforcement—Judge Ginsburg pointed out that "the whole of one's movements over the course of a

164. United States v. Jones, 132 S.Ct. 945, 948 (2012).

165. *See id.* (describing how Government relied on evidence from GPS device to obtain Jones' indictment and conviction).

166. *Id.*

167. *Id.* at 948–49.

168. *Id.* The GPS tracking warrant issued by the district court required that the officers install the device on the car registered to Jones' wife within ten days of the date on the warrant at any location within the borders of the District of Columbia. *Id*. Unfortunately, the officers installed the device on the eleventh day and in a suburban Maryland parking lot. *Id*.

169. *Id.*

170. *Id.* at 949.

171. *Id.*

172. United States v. Maynard, 615 F.3d 544, 556–57 (D.C. Cir. 2010), *aff'd*, United States v. Jones, 132 S. Ct. 945 (2012).

month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil."[173]

Judge Ginsburg further explained that law enforcement's monitoring of a single trip to the store does not reveal much about the target; but that monitoring "the whole of one's movements"[174] by contrast paints "an intimate picture of [one's] life."[175] Because we have no reason to believe that we are under constant surveillance by any particular person or entity,[176] and out of respect for the privacy we invest in the totality of our public movements, Judge Ginsburg concluded that we enjoy a reasonable expectation that we will be free from constant government surveillance as well.[177] For these reasons, the circuit court vacated Jones's conviction,[178] holding that, although Jones

173. *Id.* at 558 (emphasis in original); *see also id.* at 563 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects, each of those movements to remain 'disconnected and anonymous.'").

174. *Id.* at 558.

175. *Id.* at 562; *see also id.* ("The difference is not one of degree, but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of like, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more."); *id.* at 563 ("[P]rolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse.").

176. In an analogous way, state harassment laws and privacy tort law have reinforced the notion that people can expect to be free from unreasonable surveillance. *See, e.g.*, Galella v. Onassis, 487 F.2d 986, 998–99 (2d Cir. 1973) (upholding injunction against a persistent paparazzo); Wolfson v. Lewis, 924 F. Supp. 1413, 1420, 1433–34 (E.D. Pa. 1996) (enjoining surveillance of a family on the grounds it was part of "a persistent course of hounding, harassment and unreasonable surveillance, even if conducted in a public or semi-public place").

177. *See Maynard*, 615 F.3d at 556 (holding that the public observation doctrine provides "only that 'a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,' not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end" (quoting United States v. Knotts, 160 U.S. 276, 281 (1983))).

178. According to its decretal paragraph, the court "reversed" Jones's conviction, but one assumes that the court intended to leave open the possibility of a retrial if the government chose to retry Jones without evidence obtained by the GPS-enabled monitoring. *See, e.g.*, *id.* at 568 ("To be sure, absent the GPS data a jury reasonably might have inferred Jones was involved in the conspiracy."). The government did indeed retry Jones without the GPS data, resulting in a mistrial. *Id.* The jury was deadlocked. David Kravets, *Alleged Drug Dealer at Center of Supreme Court GPS Case Wins Mistrial,* WIRED,

lacked a discrete Fourth Amendment interest in most of his individual public movements, he had a reasonable expectation of privacy in the total quantity of "his movements over the course of a month," which was "defeated" by law enforcement's "use of the GPS device."[179]

The Supreme Court affirmed unanimously.[180] The Court's opinion, written by Justice Scalia and joined by Chief Justice Roberts with Justices Kennedy, Thomas, and Sotomayor, held that the installation of the GPS device on Jones's car involved a search because it was accomplished by a trespass for the purpose of obtaining information.[181] Although the investigating officers had a warrant, they violated its terms, rendering the installation unreasonable.[182] The majority left for another day the question of whether monitoring of Jones's movements using the GPS device raised any additional Fourth Amendment issues.[183] The concurring opinions, however, left little doubt about which view the Court will take when that day comes.[184]

For himself and Justices Ginsburg, Breyer, and Kagan, Justice Alito concurred in *Jones* to express his skepticism of the majority's trespass-based holding and his preference for a quantitative approach to evaluating Fourth Amendment priva-

Mar. 4, 2013, *available at* http://www.wired.com/threatlevel/2013/03/gps-drug-dealer-retrial/. In May 2013 Jones Agreed to a plea deal with prosecutors for a 15 year sentence with credit for time served. Nick Anderson & Anne E. Marimow, *Former D.C. Nightclub Owner Antoine Jones Sentenced on Drug Charge*, WASH. POST, May 1, 2013, http://failover.washingtonpost.com/local/antoine-jones-pleads-guilty-to-drug-charge/2013/05/01/1109c268-b274-11e2-bbf2-a6f9e9d79e19_story.html.

179. *Maynard*, 615 F.3d at 563.

180. Jones v. United States, 132 S. Ct. 945, 954 (2012).

181. *Id.*; *see also* United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) ("When the Government *does* engage in a physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment."). During the October 2012 term, the Court confirmed its commitment to preserving physical intrusion as a baseline for determining whether law enforcement conduct constitutes a "search." *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

182. *Maynard*, 615 F.3d at 566–67. *Cf.* United States v. Johnson, 333 U.S. 10, 13–14 (1948) (holding that, absent emergency or other exceptional circumstance, the Fourth Amendment requires that determinations of reasonableness be made by a judicial officer rather than "zealous officers" who are "engaged in the often competitive enterprise of ferreting out crime"). Judge Kavanaugh proposed trespass as a narrower ground for decision in his dissent from the Circuit Court's denial of the petition for rehearing en banc. *See* United States v. Jones, 625 F.3d 766, 769–71 (2010) (Kavanaugh, J., dissenting).

183. *Jones*, 132 S. Ct. 945 (2012).

184. *Id.* at 954–64.

cy interests in the face of new surveillance technologies.[185] For Justice Alito, the driving concern raised by emerging surveillance technologies is scale.[186] "In the pre-computer age," he points out, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[187] Long-term surveillance by traditional means was logistically difficult and prohibitively expensive.[188] Its rarity provided citizens with good reason to expect that they would generally be free from surveillance, and could enjoy a substantial degree of anonymity in the aggregate of their public activities.[189] Although "short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," Justice Alito would have held that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[190]

Courts and scholars have described the case-by-case method of evaluating quantitative privacy advocated by Judge Ginsburg and Justice Alito as the "mosaic" theory.[191] The critical question under this approach is whether the collection of personal information aggregated by officers during a given investigation violates reasonable expectations of privacy. Responding to that question on the record before him in *Jones*, Justice Alito declined to "identify with precision the point at which the tracking of [Jones's] vehicle became a search," but thought it clear that "the line was surely crossed before the 4-week mark."[192]

Justice Sotomayor wrote a separate concurrence in *Jones* to express her support for the majority's ruling and her sympa-

185. *Id.* at 957–58 (Alito, J., concurring).

186. *Id.* at 963–64.

187. *Id.* at 963.

188. *Id.*

189. *Id.* at 963–64. *See also* Hutchins, *supra* note 135, at 455–56.

190. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring); *see also* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 547–48 (2005).

191. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd*, United States v. Jones, 132 S. Ct. 945 (2012); Kerr, *supra* note 33, at 313. The term "mosaic" is borrowed from national security law, where the Government has defended against requests made under the Freedom of Information Act on the grounds that when otherwise innocuous intelligence information is aggregated it can reveal secret methods and sources. *See generally* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

192. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

thy with Justice Alito's quantitative approach to Fourth Amendment privacy.[193] In terms familiar to information privacy law scholars, she explained that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[194] Because it "mak[es] available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," she worried that it is "susceptible to abuse."[195]

Further, and echoing concerns expressed by the Information Privacy Law Project, Justice Sotomayor was troubled that broad deployment of modern tracking technology would "chill[] associational and expressive freedoms," while "alter[ing] 'the relationship between citizen and government in a way that is inimical to a democratic society.'"[196] In addition to modifying the public observation doctrine, Justice Sotomayor suggested that providing full protection for Fourth Amendment interests in quantitative privacy may also require "reconsider[ing]" the third-party doctrine to prevent the government from simply using private agents to conduct indirectly surveillance that it cannot pursue directly.[197]

The worries expressed by the concurring Justices in *Jones* resonate strongly with work done by information privacy law scholars that explains the value of quantitative privacy for liberty and democracy.[198] Although there have until now been very few connections drawn between information privacy law and Fourth Amendment theory and doctrine, the concurring opinions in *Jones* suggest that these days of isolation are over.[199] There is, of course, a considerable amount of work that remains to be done.[200] Among the many challenges issued by critics on

193. *Id.* at 954–57 (Sotomayor, J., concurring).

194. *Id.* at 955.

195. *Id.* at 956.

196. *Id.* (Flaum, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 286 (2011)); *see also* Richards, *supra* note 39, at 1087, 1102–03.

197. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). *See generally* Mary Leary, *The Missed Opportunity of* United States v. Jones*—Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331 (2012) (arguing for legislation constraining private entities from gathering and analyzing personal data).

198. Richards, *supra* note 40, at 1935, 1945–49; Leary, *supra* note 197, at 351–54.

199. *Jones*, 132 S.Ct. at 954–64.

200. *See generally* Kerr, *supra* note 33, 328–43.

and off the Court is whether quantitative privacy and the interests it protects have real Fourth Amendment salience.[201] We answer that challenge in the next section.

C. THE FOURTH AMENDMENT FOUNDATIONS OF QUANTITATIVE PRIVACY

Although the value placed in quantitative privacy by information privacy law scholars, practitioners, and advocates has not yet played a prominent role in Fourth Amendment doctrine, the foundations are there.[202] The Fourth Amendment was conceived, and has long served, as a bulwark against law enforcement's teleological tendency toward a surveillance state.[203] So too does the Fourth Amendment—on its own and in a broader constitutional context—treat privacy as essential to liberty and a functioning democracy.[204] Together, these established Fourth Amendment values provide ample ground for extending Fourth Amendment protections to cover reasonable expectations of quantitative privacy.[205]

Like many provisions in the Bill of Rights,[206] the Fourth Amendment's prohibition on unreasonable searches and seizures and its limitations on warrants have a reactionary origin story.[207] The core text of the Constitution does not provide for individual rights.[208] Although this omission was criticized during the drafting process,[209] it received particular attention dur-

201. *Id.* at 315, 343–45.

202. *See generally* Richards, *supra* note 39.

203. Davies, *supra* note 42, at 590 (arguing that the framers' target when adopting the Fourth Amendment was broad and indiscriminate search programs granting unbounded discretion to executive agents, including general warrants, which "undermine the right of security in person and house").

204. Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 340–45 (2010).

205. *Cf.* Leary, *supra* note 197, at 351–54 (stating legislative protections for quantitative privacy should be enacted).

206. Davies, *supra* note 42, at 673.

207. *See* NELSON B. LASSON, THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 13, 51–78 (1937); Thomas R. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 980 (2011); Davies, *supra* note 42, at 561–67, 673–74.

208. *See* LASSON, *supra* note 207, at 83.

209. *See, e.g.*, *id.* at 84–86; George Mason, Objections to the Constitution of Government Formed by the Convention 1–2 (1787) (unpublished manuscript) available at http://virginiamemory.com/docs/hires/masonobjections/pdf (complaining about the absence of a "Declaration of Rights" in the Constitution and expressing concerns that this omission would effectively moot the declarations of rights found in the constitutions of the states).

ing ratification when state legislatures raised concerns about the tyrannical potential of a strong federal government.[210] Their fears were not abstract.[211] Members of these legislatures and their constituents still bore the scars of constraint and disfavor at the hands of the Crown and shared a common law consciousness shadowed by the Star Chamber and the torturous abuses of the Tower and the Church.[212] It was against these archetypes of tyranny that the Bill of Rights was drafted and adopted.[213]

The Fourth Amendment drew on these historical experiences to describe limitations on "the amount of power that [our society] permits its police to use without effective control by law."[214] During the colonial period, British officials and their representatives took advantage of writs of assistance and other general warrants, which immunized them from legal liability for their invasions,[215] in order to search anyone they pleased, anywhere they pleased, without having to specify cause or reason.[216] James Otis, who famously vacated his office as Advocate

210. *See* LASSON, *supra* note 207, at 83, 87–97; Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 400 (1974) ("To be sure, the framers appreciated the need for a powerful central government. But they also feared what a powerful central government might bring, not only to the jeopardy of the states but to the terror of the individual."); Clancy, *supra* note 207, at 1034–36.

211. LASSON, *supra* note 207, at 13, 51–78.

212. *See* LASSON, *supra* note 207, at 24–28, 32; Clancy, *supra* note 207, at 981, 103–44; *c.f.* Warden v. Hayden, 387 U.S. 294, 313 (1967) (Douglas, J., dissenting) (discussing historical abuses of writs); Ker v. California, 374 U.S. 23, 62 n.15 (1963) (Brennan, J., dissenting) (same); Frank v. Maryland, 359 U.S. 360, 375 (1959) (same).

213. *See* LASSON, *supra* note 207, at 13–50; Clancy, *supra* note 207, at 1002–04.

214. Amsterdam, *supra* note 210, at 377.

215. *See* Amar, *supra* note 132, at 767, 774; VA. DECL. OF RIGHTS, art. X (defining "general warrants" as warrants "whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence"). For an example of a writ of assistance and the contemporary judicial decisions defending them, see 5 PHILIP KURLAND & RALPH LERNER, THE FOUNDERS' CONSTITUTION 223–24 (2000).

216. LASSON, *supra* note 207, at 51–78; TEDFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 24–46 (1969); *see* Amsterdam, *supra* note 210, at 367, 388–89, 398; Clancy, *supra* note 207, at 1002–04; Crocker, *supra* note 204, at 350–53*; see also* United States v. Poller, 43 F.2d 911, 914 (2d Cir. 1930) ("[T]he real evil aimed at by the Fourth Amendment is the search itself, that invasion of a man's privacy which consists in rummaging about among his effects to secure evidence against him").

General when solicited to defend writs of assistance, described general warrants in a 1761 court argument as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book."[217] Among those in the audience for Otis's speech was a young attorney named John Adams, who would later be a principal contributor to the text of the Fourth Amendment.[218] It is therefore no surprise that the Fourth Amendment prohibits "unreasonable searches and seizures" and insists upon warrants issued only "upon probable cause, supported by Oath or affirmation, and particularly de-

217. James Otis, *Against Writs of Assistance*, *in* AMERICAN SPEECHES; THE REVOLUTION TO THE CIVIL WAR (Ted Widner ed. 1st ed. 2006). Otis' objections to writs of assistance as a form of general warrant focused on breadth and scope, their inability to limit the discretion of officers who would become petty tyrants, and the authority to delegate search responsibilities to others, who in turn might act as tyrants.

> In the first place, the writ is UNIVERSAL, being directed "to all and singular justices, sheriffs, constables and all other officers and subjects &c." so that, in short, it is directed to every subject in the King's dominions; every one with this writ may be a tyrant; if this commission be legal, a tyrant may in a legal manner, also, control, imprison or murder any one within the realm.
>
> In the next place, IT IS PERPETUAL; there's no return, a man is accountable to no person for his doings, every man may reign secure in his petty tyranny, and spread terror and desolation around him, until the trump of the arch angel shall excite different emotions in his soul.
>
> In the third place, a person with this writ, in the daytime, may enter all houses, shops, &c., AT WILL, and command all to assist him.
>
> Fourth, by this not only deputies, etc., but even their THEIR MENIAL SERVANTS, ARE ALLOWED TO LORD IT OVER US— What is this but to have the curse of Canaan with a witness on us, to be the servants of servants, the most despicable of God's creation?

Id. at 3. As an example of how the authority provided by general warrants can be abused, Otis then goes on to recount an episode where a certain Mr. Ware retained delegated authority under a general warrant held by a Mr. Pew. When Ware was hailed into court to answer an unrelated charge for breach of the Sabbath, he used the warrant as a license to seek revenge against the constable who arrested him and the judge who presided over his case by subjecting both of their homes to lengthy and invasive searches "from the garret to the cellar." *Id*. at 3–4. Otis's views were well-founded in the English common law of the time. *See* Davies, *supra* note 42, at 562–63.

218. Clancy, *supra* note 207, at 979 ("Most of the language and structure of the Fourth Amendment was primarily the work of one man, John Adams."). Responsibility for drafting the text of the Fourth Amendment for the First Congress fell to James Madison. Davies, *supra* note 42, at 693–94. There is no contest, however, that the final text, in both content and structure, was deeply affected by Article XIV of the Massachusetts Declaration of Rights, which was drafted by Adams. Clancy, *supra* note 207, at 980–81.

scribing the place to be searched, and the persons or things to be seized."[219]

Although the negative rights afforded by the Fourth Amendment have specific historical antecedents, the text itself evinces a broader historical purpose to protect against indiscriminate and invasive governmental practices that are characteristic of a surveillance state.[220] The protections belong to individuals and to society as a whole.[221] As Anthony Amsterdam reports, early English judges saw indiscriminate searches as offenses not just against individuals, but against the "whole English nation."[222] For example, instructing the jury in *Wilkes v. Wood*—one of the cases widely credited as a guidepost for those who wrote and ratified the Fourth Amendment—Chief Justice Pratt warned that, if the power to engage in broad searches and seizures "is truly invested in the secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject."[223] The Fourth

219. U.S. CONST. amend. IV; *see* Amsterdam, *supra* note 210, at 388–89; Clancy, *supra* note 207, at 152–53; Davies, *supra* note 42, at 585, 609, 643–44; *see also* TAPAC, *supra* note 83, at 22 ("One of the colonists' most potent grievances against the British government was its use of general searches. The hostility to general searches found powerful expression in the [Fourth Amendment to the] U.S. Constitution.").

220. *See* United States v. Di Re, 332 U.S. 581, 595 (1948) ("But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment."); Johnson v. United States, 333 U.S. 10, 14 (1948) ("The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance."); Amsterdam, *supra* note 210, at 366 ("Looking back to . . . the specific incidents of Anglo-American history that immediately preceded the adoption of the amendment, we shall find that the primary abuse thought to characterize the general warrants and the writs of assistance was their indiscriminate quality, the license that they gave to search Everyman without particularized cause.").

221. *See supra* note 220.

222. Amsterdam, *supra* note 210, at 366 n.192.

223. 4 WILLIAM BLACKSTONE, COMMENTARIES 288 (1768) ("A *general* warrant to apprehend all persons suspected, without naming or particularly describing any person in special, is illegal and void for it's uncertainty; for it is the duty of the magistrate, and ought not to be left to the officer, to judge of the ground of suspicion."); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L. J. 393, 399 (1995) (quoting Wilkes v. Wood, 19 Howell's State Trials 1153, 1157 (C.P. 1763)); *see also* Grumon v. Raymond, 1 CONN. 40 (1814) ("[T]he law knows of no such process as one to arrest all suspected persons, and bring them before a court for trial. It is an

Amendment reflects this societal focus by securing to "the people" the right against unreasonable search and seizure.[224] The Court's exclusionary rule jurisprudence enforces these broad protections by punishing law enforcement in individual cases in order to effect general deterrence against future violations.[225] Thus, as Renée Hutchins has pointed out, "[t]he Fourth Amendment . . . erects a wall between a free society and overzealous police action—a line of defense implemented by the framers to protect individuals from the tyranny of the police state."[226]

Bear in mind that the tyranny that inspired adoption of the Fourth Amendment is not necessarily the product of evil intent.[227] Rather, tendencies toward a surveillance state are part of the very purpose of law enforcement.[228] Efforts to ensure

idea not to be endured for a moment. It would open a door for the gratification of the most malignant passions, if such process issued by a magistrate should skreen him from damages."); Huckle v. Money, [1763] 95, Eng. Rep. 768 (K.B.) 769 ("To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour . . . .").

224. U.S. CONST. amend IV; *see* United States v. White, 401 U.S. 745, 760 (1971) (Douglas, J., dissenting) ("Today no one perhaps notices because only a small, obscure criminal is the victim. But every person is the victim, for the technology we exalt today is everyman's master."); Crocker, *supra* note 204, at 309–10, 360; Kathleen M. Sullivan, *Under a Watchful Eye: Incursions on Personal Privacy*, *in* THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM 129 (Richard C. Leone & Greg Anrig eds., 2003) ("By permitting searches and seizures only if reasonable, and interposing the courts between the privacy of citizens and the potential excesses of executive zeal, these constitutional protections" help to protect against "dragnets, or general searches, which were anathema to the colonists who rebelled against the British crown.").

225. *See* Davis v. United States, 131 S. Ct. 2419, 2426 (2011) ("The rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations."); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1263–72 (1982). For a critique of the deterrence approach to justifying the Fourth Amendment exclusionary rule, see David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence,* 50 AM. CRIM. L. REV. 1 (2013) and David Gray et al., *The Supreme Court's Contemporary Silver Platter Doctrine,* 91 TEX. L. REV. 7 (2012).

226. Hutchins, *supra* note 135, at 444. *But see* Davies, *supra* note 42, at 641 ("The principal historical complaint regarding constables was not their overzealousness so much as their inaction.").

227. *See* KURLAND, *supra* note 215, at 223–24.

228. *See* Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971); James Madison, *Speech at the First Congress, First Session: Amendments to the Constitution* (June 8, 1789), *in* 5 WRITINGS OF JAMES MADISON 374–75 (Gaillard Hunt ed., 1904) (worrying that, absent specific constraint, the federal govern-

peace and security naturally impel the state toward the most expansive and efficient means of detecting and preventing crime.[229] In this sense, "The Bill of Rights in general and the Fourth Amendment in particular are profoundly anti-government documents [in that] [t]hey deny to government . . . desired means, efficient means . . . to obtain legitimate and laudable objectives."[230] But the constraint is necessary because law enforcement, *qua* law enforcement, will naturally seek every advantage it can to catch criminals without necessarily considering the broader consequences for liberty and democracy.[231] Reduced to a phrase familiar to every student of elementary school civics, this is the Fourth Amendment's critical role in our constitutional system of checks and balances.

The specters of a tyrannical surveillance state that plagued our founding-era forebears no doubt warranted constitutional attention.[232] They lived in a world in which executive agents kicked down doors, entered homes, and rummaged through drawers at will.[233] Law-abiding citizens might have hoped that they were immune from such intrusions, but that would have been naïve.[234] A state interested in maintaining its own authority and ensuring maximum security is not so discriminate.[235] As

ment would revert to the use of general warrants under the "necessary and proper clause").

229. *See* Balkin, *supra* note 17, at 3–4; Amsterdam, *supra* note 210, at 378–79.

230. Amsterdam, *supra* note 210, at 353.

231. *See* Johnson v. United States, 333 U.S. 10, 14 (1948); BAMFORD, SHADOW, *supra* note 6, at 111 (describing how NSA surveillance efforts have expanded rapidly during the cold war and in the wake of the terrorist attacks of September 11, 2001, "due to limited outside oversight" because it "wanted to be able to target thousands of people simultaneously, some briefly and some long term, without the hassle of justifying them to anyone higher than an anonymous shift supervisor").

232. *See* Madison, *supra* note 228, at 374; Otis, *supra* note 217, at 1–5.

233. Entick v. Carrington, 19 Howell's State Trials 1029 (C.P. 1765) provided another pre-revolutionary example of what life in such a state might look like. There, Chief Justice Camden famously wrote that the common law of England prohibited indiscriminate governmental trespass upon private property and that such invasions could only be justified "by public law" and "for the good of the whole." *Id.*

234. *See* Madison, *supra* note 228, at 374–75.

235. *See* John F. Mercer, *Essays by a Farmer*, MARYLAND GAZETTE (Feb. 15, 1788) reprinted in THE COMPLETE ANTI-FEDERALIST (Herbery J. Storind ed. 1981) ("[S]uppose for instance, that an officer of the United States should force the house, the asylum of a citizen, by virtue of a general warrant, I would ask, are general warrants illegal by the constitution of the United States? Would a court, or even a jury, but juries are no longer to exist, punish a man

our founders learned, it will cut a broad swath, targeting not only criminals but also eccentrics and troublemakers, including political activists, academics, artists, and promoters of disfavored religions.[236] Today we are relearning the same lesson as government search programs target everyone who makes phone calls or uses the Internet.[237]

As William Stuntz has pointed out, it was precisely these broad government attacks on speech and conscience in the context of heresy and sedition cases that informed the substantive character of the Fourth Amendment at its inception.[238] As we discussed in Part I, the threat of surveillance is a powerful tool for modifying behavior as well as character.[239] Thus illuminated, the Fourth Amendment is revealed as playing a critical role in our system of constitutional protections because it prohibits the kinds of broad programs of indiscriminate search that might render docile a people defined by their spirit of liberty.[240]

---

who acted by express authority, upon the bare recollection of what once was law and right? I fear not, especially in those cases which may strongly interest the passions of government, and in such only have general warrants been used.").

236. Individuals in these categories have always been the natural targets of tyranny. The certainly were in the founding era. *See* Crocker, *supra* note 204, at 346–50. Writs of assistance in the colonies were little more than protection of petty tyrants, who sometimes used them to retaliate against outspoken citizens. *See* LASSON, *supra* note 207, at 59–60. Things have not changed significantly since. Abusive regimes from Asia to Africa to Europe to South America have put political opponents, intellectuals, artists, and religious leaders under surveillance, or worse. JEAN-PAUL BRODEUR & STEPHANIE LEMAN-LANGLOIS, THE NEW POLITICS OF SURVEILANCE AND VISIBILITY 183–90 (Richard Ericson & Kevin D. Iagerty eds., 2006). The same impulses of distrust are suffused through our politics. Nixon bugged not drug lords but the headquarters of his political rivals and civil rights agitators. Nat Hentoff, *Forty Years of Growing Surveillance*, N.Y. TIMES, June 13, 2012, http://www.nytimes.com/roomfordebate/2012/06/13/did-any-good-come-of-watergate/since-watergate-government-surveillance-is-more-sophisticated.

237. These are, of course, the groups targeted by recently revealed surveillance programs directed by the FBI and NSA. *See supra* notes 1–6, 82–85 and accompanying text.

238. Stuntz, *supra* note 223, at 394.

239. *See* Cohen, *supra* note 90, at 1425–26.

240. *See* Crocker, *supra* note 204, at 360; *see also* Florida v. Riley, 488 U.S. 445, 466–67 (1989) (Brennan, J., dissenting) ("The Fourth Amendment demands that we temper our efforts to apprehend criminals with a concern for the impact on our fundamental liberties of the methods we use. I hope it will be a matter of concern to my colleagues that the police surveillance methods they would sanction were among those described 40 years ago in George Orwell's dread vision of life in the 1980's . . . ."); BAMFORD, SHADOW, *supra* note 6, at 31 (quoting NSA head Michael Hayden's comments on the movie *Enemy of the State*: "But I'm not too uncomfortable with a society that makes its boo-

The concerns about broad programs of indiscriminate search that drove us to adopt the Fourth Amendment in 1791 are raised anew with law enforcement's unfettered access to contemporary surveillance technologies.[241] The stakes are profound. Should law enforcement have unrestricted access to technologies like GPS-enabled tracking, drones, and massive data aggregation systems capable of effecting broad and indiscriminate surveillance of all of us, all of the time, across every dimension of our daily lives? Or, in the alternative, does the Fourth Amendment guarantee to all of us and to each of us the right not to live in this kind of surveillance state? As we see it, the Fourth Amendment's text, history, and doctrine leave no doubt that it is the latter.[242]

The governing standard for determining whether law enforcement conduct constitutes a Fourth Amendment "search" is described by Justice Harlan in his concurring opinion in *United States v. Katz*.[243] Under the *Katz* inquiry, the Court will recognize a subjectively manifested expectation of privacy as "rea-

geyman secrecy and power. That's really what the movie's about—it was about the evils of secrecy and power . . . making secrecy and power the boogeymen of political culture, that's not a bad society"); *cf.* Lawrence v. Texas, 539 U.S. 558, 562 (2003) ("Liberty protects the person from unwarranted government intrusions into a dwelling place or other private places . . . . Liberty presumes an autonomy of the self that includes freedom of thought, belief, expression, and certain intimate conduct."). Alas, there is already evidence that the surveillance state initiated in the United States over the course of the last decade has produced precisely this sort of docility, which we feel certain our forefathers would have deplored. In a recent Pew Research Center poll seeking reactions to recent revelations about surveillance programs operated by the FBI and NSA, fifty-six percent of respondents thought it was "acceptable" that the "NSA [is] getting secret court orders to track calls of millions of Americans to investigate terrorism." PEW RESEARCH CTR., MAJORITY VIEWS NSA PHONE TRACKINGS AS ACCEPTABLE ANTI-TERROR TACTIC 2 (June 10, 2013). Fortunately, the Fourth Amendment stands as a bulwark against docility as well. *See* Davies, *supra* note 42, at 657–60. The very function of constitutionally guaranteed rights in a constitutional democracy is to prevent the degradation of those rights by inattention or even by democratic means. *Id.*

241. *See* Berger v. New York, 388 U.S. 41, 64 (1967) (Douglas, J., concurring) ("I also join the opinion because it condemns electronic surveillance, for its similarity to the general warrants out of which our Revolution sprang and allows a discreet surveillance only on a showing of 'probable cause.'"); TAPAC, *supra* note 83, at 35 ("The greatest risk of government data mining is that access to individually identifiable data chills individual behavior . . . . This helps explain the constitutional hostility to general searches—to government surveillance without individualized suspicion—by the government.").

242. *See supra* notes 220–23 and accompanying text.

243. Katz v. United States, 389 U.S. 347, 359–61 (1967) (Harlan, J., concurring).

sonable" if it is an expectation that is broadly shared by most citizens, realistic in light of common social practices, and threatened by unfettered governmental intrusion.[244] From an ethnographic point of view, it is hard to contest Renée Hutchins's observation that "citizens of this country largely expect the freedom to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings."[245] There is no doubt that technology capable of pervasive monitoring implicates those reasonable and generally held expectations of privacy.[246] Anthony Amsterdam perhaps put it best, writing that "[t]he insidious, far-reaching and indiscriminate nature of electronic surveillance—and, most important, its capacity to choke off free human discourse that is the hallmark of an open society—makes it almost, although not quite, as destructive of liberty as 'the kicked-in door.'"[247]

* * *

In Part I, we explored how information privacy scholarship has provided theoretical and practical justifications for the proposition that we can and should maintain expectations of privacy in large quanta of personal information. In this Part, we demonstrated that the fundamental concerns for liberty and democracy that lie at the heart of this work illuminate Fourth Amendment concerns expressed by the concurring opinions in *United States v. Jones*. The next question, then, is how to translate the Fourth Amendment imperative to protect reasonable expectations in quantitative privacy into practice.[248] We take up that challenge in the next Part.

244. *See id.* at 361; *see also* California v. Ciraolo, 476 U.S. 207, 211–12 (1986) (applying the social inquiry prong of justice Harlan's reasonable expectations of privacy test).

245. Hutchins, *supra* note 135, at 455; s*ee also* Jones v. United States, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring); *id.* at 963–64 (Alito, J., concurring). One might argue that, as a descriptive matter, emerging surveillance technologies make it unreasonable to expect this level of privacy. As we argue below, this amounts to "technological determinism run amok." *See infra* notes 387–92 and accompanying text.

246. United States v. White, 401 U.S. 745, 759–60 (1971) (Douglas, J., dissenting) ("Electronic aids add a wholly new dimension to eavesdropping. They make it more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny." (quoting Lopez v. United States, 373 U.S. 427, 439 (1963) (Brennan, J., dissenting)).

247. Amsterdam, *supra* note 210, at 388.

248. Balkin, *supra* note 17, at 23; Kerr, *supra* note 33, at 330–54.

III. THE TECHNOLOGY-CENTERED APPROACH TO QUANTITATIVE PRIVACY

Fourth Amendment debates about quantitative privacy have so far been dominated by discussion of the "mosaic" theory.[249] Under the mosaic theory, Fourth Amendment interests would be determined on a case-by-case basis by assessing the quality and quantity of information about a suspect gathered in the course of a specific investigation.[250] The United States Court of Appeals for the District of Columbia adopted this approach in the predecessor to *Jones*.[251] The concurring opinions in *Jones* also appear to endorse the mosaic theory.[252] In the months after *Jones*, prominent quantitative privacy advocates have come forward to expand, explore, and defend the mosaic approach.[253] At the same time, the mosaic approach has been a target for pointed criticism on both doctrinal and practical grounds.[254] We think that the Fourth Amendment and the privacy issues at stake, as we have described them here, suggest taking a different tack.

In our view, the threshold Fourth Amendment question raised by quantitative privacy concerns is whether an investigative technique or technology has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government.[255] There are a number of ways that the Fourth Amendment status of a surveillance technique or technology could be determined. The most obvious would be for anyone who knows that he or she has been subject to surveillance by a novel technology, or dramatically improved existing technology, to file a civil suit seeking equitable relief or even damages.[256] In such an ac-

249. *See, e.g.*, *Jones*, 132 S. Ct. at 953–54; Kerr, *supra* note 33, at 330–54; Slobogin, *supra* note 53, at 3.

250. *See, e.g.*, Slobogin, *supra* note 53, at 3.

251. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd* United States v. Jones, 132 U.S. 945 (2012).

252. *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring); *id*. at 964 (Alito, J., concurring).

253. *See, e.g.*, Slobogin, *supra* note 53, at 3–4, 12–23.

254. *See, e.g.*, *Jones*, 132 S. Ct. at 953–54; Kerr, *supra* note 33, at 330–54.

255. *See* Freiwald, *supra* note 41, at 15–18 (arguing for a Fourth Amendment focus on surveillance technologies).

256. *See, e.g.*, Clapper v. Amnesty Int'l, 133 S. Ct. 1338 (2013) (holding that Article III requires that a party seeking to challenge the constitutionality of the Foreign Intelligence Surveillance Act (FISA) or executive conduct licensed by the Foreign Intelligence Surveillance Court (FISC) must have actual

tion, a court would first need to determine whether the technology at issue should be subject to Fourth Amendment regulation. Among the important factors that a court would need to consider are: (1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs associated with deploying and using the technology. If a court finds that a challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use, then granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy.[257]

The critical goal, of course, will be to tailor an approach that satisfies Fourth Amendment standards by reflecting a clear understanding and appreciation of both the law enforcement and privacy interests at stake.[258]

Once a surveillance technology has been identified as implicating the Fourth Amendment, and a reasonable approach to limiting law enforcement's access and discretion has been devised, subsequent litigants would have the option of challenging law enforcement's conformance with the regulatory scheme (be it a warrant regime or some other means), the constitutionality of law enforcement's conduct regardless of the scheme, or both. For students of criminal procedure, there is no surprise here. After all, defendants subject to physical searches of their homes are at liberty to challenge the constitutionality of local warrant procedures,[259] the constitutionality of a warrant,[260] and

knowledge that he, she, or it is subject to surveillance under FISA, an order of the FISC, or both, in order to establish standing). Although it is not necessary to our argument here, we see no reason why any citizen could not bring a Fourth Amendment claim challenging law enforcement's unfettered access to a surveillance technology or the Fourth Amendment sufficiency of a legislative or executive regulatory scheme governing law enforcement's access to a surveillance technology. After all, each of us has an equal share in the right of the people to be secure from the vagaries of a surveillance state.

257. *See supra* Parts I–II.

258. In other work, we have described in detail and at length some of the law enforcement interests served by many emerging surveillance and data aggregation technologies. *See generally* Gray, Citron & Rinehart, *supra* note 25.

259. *See, e.g.*, Connally v. Georgia, 429 U.S. 245, 246 (1977) (challenging constitutionality of local procedure whereby magistrates were only paid if they issued a warrant); Coolidge v. New Hampshire, 403 U.S. 443, 449 (1971) (challenging local practice of allowing law enforcement officials to issue warrants).

260. *See, e.g.*, Winston v. Lee, 470 U.S. 753, 755 (1985) (challenging warrant for licensing overly invasive search); Andresen v. Maryland, 427 U.S. 463,

even the constitutionality of law enforcement's conduct during a warranted search.[261] Thus, although the technology-centered approach to conceptualizing and defending Fourth Amendment rights to quantitative privacy proposed here is novel, its application would not require straying from well-traveled litigation pathways.

In this Part, we elaborate further how this technology-centered approach would work in practice by considering how it would apply to emerging surveillance technologies, such as aerial drones, GPS-enabled tracking, the NSA's telephonic and data surveillance programs, and the NYPD's Domain Awareness System, and how it would apply to traditional investigative methods like human surveillance. We begin by explaining the Fourth Amendment pedigree of our technology-centered approach.

A. FOURTH AMENDMENT PRECEDENTS FOR A TECHNOLOGY-CENTERED APPROACH

The Fourth Amendment guards against the government's unfettered use of techniques and technologies that raise the specter of a surveillance state.[262] For our forebears, those fears arose in reaction to the broad and indiscriminate use of physically invasive searches and seizures.[263] Today, the risk of a surveillance state arises with law enforcement's unfettered access to advanced surveillance technologies, including aerial drones, GPS-enabled tracking devices, and data aggregation and min-

465 (1976) (challenging warrant for licensing overbroad search).

261. *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 929 (1995) (challenging law enforcement's failure to "knock and announce" when conducting a warranted search); Hummel-Jones v. Strope, 25 F.3d 647, 650 (8th Cir. 1994) (challenging length of time individuals on the scene of a warranted search were detained).

262. *See generally* Crocker, *supra* note 204.

263. Stuntz, *supra* note 223, at 402–03 (1995). *See also* Davies, *supra* note 42, at 578–82, 736 ("The common-law tradition viewed any form of discretionary authority with unease—but delegation of discretionary authority to ordinary, 'petty,' or 'subordinate' officers was anathema to framing-era lawyers;" and "[the Framers] banned general warrants in order to prevent the officer from exercising discretionary authority."); James Madison, *Amendments to the Constitution* (June 8, 1789), *in* 12 THE PAPERS OF JAMES MADISON 197, 205 (Robert A. Rutland et al. eds., 1979) ("It is true the powers of the general government are circumscribed; they are directed to particular objects; but even if government keeps within those limits, it has certain discretionary powers with respect to the means, which may admit of abuse to a certain extent, in the same manner as the powers of the state governments under their constitutions may to an indefinite extent.").

ing projects like DAS, fusion centers, and NSA's telephonic and data surveillance programs.[264] In her concurring opinion in *Jones*, Justice Sotomayor highlighted the democratic consequences of these technologies, which can capture "at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track."[265] The Information Privacy Project's concerns animate Justice Sotomayor's concurrence in *Jones*. Informed by the project's work, we see strong Fourth Amendment grounds for regulating government's access to and use of investigative technologies that are capable of broad and indiscriminate data collection, data retention, data analysis, and direct monitoring because they are "inimical to democratic society."[266]

Although it has not squarely addressed the issue, existing Supreme Court doctrine exhibits considerable sympathy for the proposition that emerging technologies capable of amassing large quantities of information about individuals implicate Fourth Amendment bulwarks against a surveillance state.[267] In

264. *Cf.* United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting) ("What the ancients knew as 'eavesdropping,' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb. Electronic surveillance is the greatest leveler of human privacy ever known. . . . [T]he concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on.").

265. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

266. *Id.*

267. *See, e.g.*, United States v. U.S. Dist. Ct., 407 U.S. 297, 312–13 (1972) ("[A] recognition of these elementary truths does not make employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy . . . . [*Katz*] implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." (citations omitted)); White, 401 U.S. at 760 (Douglas, J., dissenting) ("I would stand by *Berger* and *Katz* and reaffirm the need for judicial supervision under the Fourth Amendment of the use of electronic surveillance which, uncontrolled, promises to lead us into a police state." (citation omitted)); Berger v. New York, 388 U.S. 41, 64 (1967) ("[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments." (quoting Lopez v. United States, 373 U.S. 427, 441 (1963)

the years since the Fourth Amendment was ratified in 1791, courts routinely have been called upon to evaluate the potential of emerging investigative techniques and technologies to diminish privacy.[268] When unfettered access to those methods raises the specter of a surveillance state, courts have limited their use by applying the Fourth Amendment's reasonableness standards.[269] For example, in *United States v. Knotts*,[270] the Court indicated that "dragnet type law enforcement practices" might threaten broadly held privacy expectations.[271] The technological capacity to effect pervasive surveillance was also at issue in *United States v. Kyllo*, which concerned the use of a heat detection device to monitor invisible thermal emanations from a home.[272] Writing for the Court in *Kyllo*, Justice Scalia emphasized that the Court must not "permit police technology to erode the privacy guaranteed by the Fourth Amendment,"[273] including existing technologies and "more sophisticated systems that are already in use or in development."[274]

Our technology-centered approach to protecting quantitative privacy follows this familiar doctrinal path, invoking the Fourth Amendment to guard against indiscriminate intrusions that compromise individuals' "power to control what others can come to know" about them.[275] In the sections that follow, we explain how that general approach would apply to investigative technologies and methods like drones, DAS, the NSA's data surveillance programs, and human surveillance.

B. THE TECHNOLOGY-CENTERED APPROACH AND AERIAL SURVEILLANCE DRONES

If an image could serve as the paradigm of the surveillance state, it would be the all-seeing government eye in the sky.[276]

(Warren, J., concurring))).

268. BREYER, *supra* note 95, at 67.

269. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001); Katz v. United States, 389 U.S. 347, 351 (1967).

270. 460 U.S. 276 (1983).

271. *Id.* at 284. For further discussion of *Knotts*, see *infra* notes 410–29 and accompanying text.

272. *See Kyllo*, 533 U.S. at 29.

273. *Id.* at 34.

274. *Id.* at 36.

275. BREYER, *supra* note 95, at 66.

276. For example, the seal for the Office of Information Awareness, which developed and operated the notorious Total Information Awareness system through the Defense Advanced Research Projects Agency, features an image of an eye atop a pyramid, similar to that which is found on the back of the one-

Drones implicate Fourth Amendment interests in quantitative privacy because they can facilitate exactly this kind of broad and indiscriminate surveillance when their deployment and use is left to the unfettered discretion of government agents. We turn first to considerations of scope. Although an individual drone can only monitor what it can see, it can see quite a lot.[277] Furthermore, unlike manned aircraft, drones can stay aloft for long periods of time, providing constant streams of information for nearly indefinite periods of time.[278] The technology is also highly scalable and increasingly inexpensive, promising an ever-expanding fleet of drones creating an ever-broadening surveillance net in the skies above us.[279] Thus, there appears to be no real limit on the breadth of surveillance that drones can accomplish.

In addition to being broad, surveillance accomplished using drones is indiscriminate in that everyone within the field of the drones' vision is under constant surveillance regardless of whether there is reason to suspect any particular person of wrongdoing. Drones are also covert by design.[280] Thus, even if some places end up being unmonitored some of the time, the ambient threat of unlimited surveillance by drones would remain ubiquitous and constant. It is hard to think of a better description of life in a surveillance state than to know that no matter where you go, and no matter when, there is an eye-in-the sky that is or may be watching you.[281] For these reasons, we

dollar bill, casting its lighted vision on the planet earth. *See* Hendrik Hertzberg, *Too Much Information*, NEW YORKER, Dec. 9, 2002, http://www.newyorker.com/archive/2002/12/09/021209ta_talk_hertzberg.

277. *See* Grossman, *supra* note 7, at 32 (reporting that the Reaper drone outfitted with a Gorgon Stare device can "surveil an area 2 ½ miles across from 12 angles at once").

278. *Id.* at 33 (reporting on one drone, the manufacturer of which "promises 'more than 21 days of unblinking stare'" and another in development that will stay aloft for five years); *see also* News Release, Northrop Grumman, Northrop Grumman Awarded $517 Million Agreement for U.S. Army Airship with Unblinking Eye, (June 14, 2010), *available at* http://www.irconnect.com/noc/press/pages/news_releases.html?d=194252.

279. *See* Grossman, *supra* note 7, at 28 (reporting that drones retail for as little as $300); *see also* Darrell Preston, *Drones Take to American Skies on Police, Search Missions*, BLOOMBERG (May 30, 2012), http://www.bloomberg.com/news/2012-05-31/drones-take-to-american-skies-on-police-search-missions.html (comparing cost of some drones to squad cars).

280. *See* Grossman, *supra* note 7, at 33 (reporting development of a "tiny drone that mimics the flight of a hummingbird").

281. *See* ORWELL, *supra* note 88, at 4 ("There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was

think that unfettered governmental access to drones subject only to the discretion of government agents implicates reasonable interests in quantitative privacy; the deployment and use of drones should therefore be subject to Fourth Amendment regulation.[282]

A determination that drones implicate Fourth Amendment interests in quantitative privacy would not bar law enforcement from using the technology. Rather, what would be prohibited is its "unreasonable" use. For Fourth Amendment purposes, "reasonableness" requires balancing the legitimate interests of law enforcement against the privacy interests of citizens.[283] Just as in more familiar Fourth Amendment contexts, applying this balancing test as part of a technology-centered approach to quantitative privacy requires finding a regulatory structure that can preserve the investigative utility of drones while minimizing their risk for abuse. What does that mean in practice?

When considering the options, it is important to distinguish between surveillance in the context of a specific investigation and ambient, general surveillance with no particular target in mind. Like physical searches, wiretapping, and GPS-enabled tracking, drones are well-suited to the surveillance of particular suspects or crimes. For example, drones might help officers track a suspect or study a crime scene.[284] By contrast, the threat to quantitative privacy posed by drones derives primarily from the prospect of their broad and indiscriminate use

guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."); *see also* Grossman, *supra* note 7, at 31 (describing the experience of being watched by a drone as "eerie, oppressive, and somewhat annoying"); INT'L HUMAN RIGHTS AND CONFLICT RESOLUTION CLINIC: STANFORD LAW SCH. & GLOBAL JUSTICE CLINIC: NYU SCH. OF LAW, LIVING UNDER DRONES: DEATH, INJURY, AND TRAUMA TO CIVILIANS FROM US DRONE PRACTICES IN PAKISTAN 80–87 (2012), *available at* http://livingunderdrones.org/wp-content/uploads/2012/10/Stanford-nyu-living-under-drones.pdf (describing the mental and emotional impact of constant drone surveillance on residents of Pakistan).

282. *See* Grossman, *supra* note 7, at 32 ("The framers didn't anticipate technology that could hover for days, keeping an eye on exposed backyards and porches, that could work in networked swarms, see through walls with thermal imaging, recognize faces and gaits and track license plates.").

283. *See* Richards v. Wisconsin, 520 U.S. 385, 394 (1997); *see also* Freiwald, *supra* note 41, at ¶ 67.

284. Christina Hernandez Sherwood, *Are You Ready for Civilian Drones?,* GOV'T TECH. MAG., Aug. 2, 2012, http://www.govtech.com/public-safety/are-you-ready-for-civilian-drones.html.

in the context of general surveillance programs. Given this dynamic, the best place to strike a reasonable balance between the privacy and law enforcement interests at stake in the use of drones is likely to be at the time of deployment. Experience with wiretapping technology provides a helpful and illuminating analogue.

Wiretapping technology has proven to be useful to law enforcement as a surveillance tool in specific investigations.[285] On the other hand, wiretapping is also capable of facilitating broad programs of indiscriminate surveillance. The Verizon order discussed above suggests that the NSA is collecting and analyzing our telephony metadata.[286] Imagine that government was also listening to the content of our telephone conversations, reminiscent of the Bush-era "Terrorist Surveillance Program."[287] There is no doubt that such a program would violate reasonable expectations of privacy protected by the Fourth Amendment precisely because it entails the broad and indiscriminate use of a surveillance technology.

To preserve reasonable expectations of privacy threatened by unfettered access to wiretapping technology, while still preserving legitimate law enforcement interests, Congress, acting in the shadow of *United States v. Katz*,[288] passed the Title III

285. Declan McCullagh, *FBI to Announce New Net-Wiretapping Push*, CNET (Feb. 16, 2011), http://news.cnet.com/8301-31921_3-20032518-281.html.

286. *See* Greenwald, *Phone Records*, *supra* note 1.

287. BAMFORD, SHADOW, *supra* note 6, at 177–96 (describing NSA's warrantless program of collecting vast streams of international and domestic e-mail and phone traffic passing through U.S. telecommunications pathways); David E. Sanger & John O'Neil, *White House Begins Effort to Defend Surveillance Program*, N.Y. TIMES, Jan. 23, 2006, http://www.nytimes.com/2006/01/23/politics/23cnd-wiretap.html?_r=1&. Congress immunized from liability the telecommunication providers involved in the TSP program. *See Congress Grants Telecommunications Companies Retroactive Immunity from Civil Suits for Complying with NSA Terrorist Surveillance Program—FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436*, 122 HARV. L. REV. 1271, 1271–72 (2009). There is indeed no assurance that the data collected through that program has been discarded. In April 2012, national security author James Bamford reported that the NSA is spending two billion dollars to construct a data center in Utah to store the information it has been collecting for the past decade. Bamford, *The NSA is Building*, *supra* note 6. According to Bamford, "[f]lowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'" *Id.*

288. 389 U.S 347, 353 (1967) (announcing that "the underpinnings of *Olmstead*," which held that wiretapping does not implicate the Fourth

Wiretap Act and then the Electronic Communications Privacy Act (ECPA).[289] Under this legislative regime, law enforcement can only use wiretapping technology if they have prior approval of a court.[290] Applications for wiretap warrants must describe the crime under investigation, identify the "communications sought to be intercepted," and provide details on where and how those communications will be intercepted.[291] A court will issue a wiretap order only where it determines that there is "probable cause for belief that an individual is committing, has committed, or is about to commit a particular [enumerated] offense;" "probable cause for belief that particular communications concerning that offense will be obtained through such interception;" and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[292] Wiretap orders must be narrowly tailored and time limited.[293] Courts also have the authority to require regular reports during the pendency of a wiretap warrant and to modify the terms as investigations unfold.[294]

This congressionally devised approach to wiretaps offers a promising model for regulating law enforcement access to other direct surveillance technologies, including drones and GPS-

Amendment because it is "surveillance without any trespass . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling," but declining to directly overrule *Olmstead* because the facts before the Court did not require doing so); *see also* United States v. Jones, 132 S. Ct. 945, 963 (2012) ("After *Katz*, Congress did not leave it to the courts to develop a body of *Fourth Amendment* case law governing [wiretapping]. Instead, Congress promptly enacted a comprehensive statute, and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law." (emphasis added) (citations omitted)).

289. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 197–239; *see also* GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING (Oct. 9, 2012), *available at* http://www.fas.org/sgp/crs/intel/98-326.pdf.

290. *See* 18 U.S.C. § 2516(1), (2) (2012).

291. *See* 18 U.S.C. § 2518(1)(b)(iii).

292. *See* 18 U.S.C. §§ 2516(1)(a)–(s), 2518(3).

293. *See* 18 U.S.C. § 2518(3), (5).

294. *See* 18 U.S.C. § 2518(6). Many of these minimization standards were hailed by the Court in *Katz* as the sorts of efforts that, if subject to prior approval of a detached and neutral magistrate, would strike a reasonable balance between law enforcement's interests in conducting electronic eavesdropping and the privacy interests threatened by this kind of surveillance. Katz v. United States, 389 U.S. 347, 354–55 (1967).

enabled tracking devices. Three features of this scheme seem particularly useful to consider. The first is its legislative provenance. Although courts are constitutionally obligated to ensure that Fourth Amendment standards are met, and any legislative scheme would ultimately be subject to court review, there is no bar on the political branches' taking the first step.[295] Justice Alito, writing for four justices in *Jones*, solicited just this kind of legislative action to regulate the use of GPS-enabled tracking technology.[296] We share his inclination, particularly in the context of emerging surveillance technologies, because the law enforcement and privacy interests at stake can be explored in a more expansive and timely manner in the context of legislative or executive rule making processes than they can be in the context of constitutional litigation.[297]

Second, the Wiretap Act only allows officers to use wiretaps during the course of specific investigations and only where there is probable cause to believe that the wiretap will produce evidence.[298] Thus, officers are provided reasonable access to the technology when and where it can advance demonstrable law enforcement interests while also securing our general expectations that government is not listening to all of our telephone conversations. This seems like a fair compromise in the context of other direct surveillance technologies like drones and GPS-enabled tracking. For example, drone surveillance might be tremendously valuable in a case like *Jones* because it would allow officers to document a suspect's pattern of travel between

295. *Cf.* Orin Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire*, 102 MICH. L. REV. 936, 943 (2004) (arguing that Congress can and should legislate on privacy rights with respect to developing technologies, rather than leaving interpretation to the courts).

296. United State v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." (citation omitted)).

297. *Id.*; *cf.* Announcement, Fed. Aviation Admin., Unmanned Aircraft Systems Test Site Selection (Feb. 14, 2013), *available at* https://faaco.faa.gov/index.cfm/announcement/view/13143 (seeking public and expert opinions on rules governing drones in domestic airspace). Two bills working their way through Congress, S. 607 (2013) and H.R. 1852 (2013), would amend the Electronic Communication Privacy Act to require that law enforcement secure a warrant based on probable cause before accessing any stored electronic communications no matter their age. Current law only requires a warrant for stored communications that are less than 180 days old. 18 U.S.C. § 2703(a).

298. *See* 18 U.S.C. § 2518(3)(b)–(c).

locations associated with a drug conspiracy.[299] Drones might serve an important purpose when used to monitor international borders.[300] In either case, requiring officers to obtain prior authorization from a court would serve legitimate law enforcement interests while also limiting access to circumstances of specific and demonstrated need.[301] That constraint would in turn preserve reasonable expectations of quantitative privacy by allowing the vast majority of us to remain secure against the prospect that law enforcement "in its unfettered discretion" was using drones or GPS-enabled tracking devices to gather "at a relatively low cost . . . a substantial quantum of intimate information"[302] about all of us all of the time.

Third, the Wiretap Act requires that courts tailor warrants and exercise appropriate supervisory authority.[303] Applied to drones, GPS-enabled tracking, and similar technologies, this requirement might mean setting limits on when, how, and how long a device can be deployed. A court might also require officers to take steps to minimize information about innocent third parties that is gathered incidentally.[304] As in all Fourth Amendment cases, the guiding principle would be to strike a reasonable balance between the investigative needs of law enforcement and the privacy interests of the suspect and society at large.[305]

299. *See generally Jones*, 132 S. Ct. at 945.

300. *See* Grossman, *supra* note 7, at 31.

301. As with physical searches, imposing a warrant-type constraint on the deployment and use of aerial drones would not bar the use of these technologies without prior court approval in emergency situations. *See* Kentucky v. King, 131 S. Ct. 1849, 1856 (2011); Brigham City v. Stuart, 547 U.S. 398, 400 (2006).

302. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

303. *See* 18 U.S.C. § 2518(6).

304. For example, wiretap orders frequently require that officers monitoring the tap make an initial assessment of relevance to their investigation and stop or erase any recordings that are not relevant. *See* 18 U.S.C. § 2518(5) (requiring minimization of interception of irrelevant information); *cf.* United States v. Padilla-Pena, 129 F.3d 457, 462 (8th Cir. 1997) (holding that interpreters that ceased translating recorded conversations after those parts already translated were found to be irrelevant comported with the level of minimization required by the wiretapping order).

305. It is no coincidence that this was precisely the approach taken during the investigation of Jones. *See Jones*, 132 S. Ct. at 948. The investigating officers sought and received a warrant to install and monitor a GPS device on Jones's car. *Id.* In keeping with habits developed in the wiretapping context, the court set limits on where and when the device could be installed and how long it could be monitored. *See id.*

In recommending some form of prior authority granted by a court as the primary tool for regulating law enforcement access to direct surveillance technology, we are far from radical. This is, after all, the primary strategy for limiting physical searches (particularly in the home), wiretaps, and searches of stored electronic communications.[306] Based on this experience, it seems that requiring officers to seek prior approval of a court before using direct surveillance technologies like aerial drones is far from unreasonable. In fact, the officers in *Jones* sought and received a warrant before installing the GPS-enabled tracking device on Jones's car.[307] They unfortunately failed to obey the terms of that warrant, but no evidence in the record suggested that it was onerous or unreasonable from a Fourth Amendment point of view to expect them to get a warrant in the first place.[308] Quite to the contrary, that is precisely what the Supreme Court ultimately required.[309] At the same time, however, it is clear that the natural impulse of government and law enforcement to expand surveillance capacities is now dominating the debate about drones.[310] Absent constitutional constraint, there may be little to protect us against skies filled with ever-watchful government eyes.

C. THE TECHNOLOGY-CENTERED APPROACH AND DATA AGGREGATION

Data aggregating and mining technologies like DAS, the NSA's telephonic and electronic surveillance programs, fusion centers, and Virtual Alabama implicate reasonable expectations of quantitative privacy principally because of their scope. Such technologies are, after all, designed to collect and analyze large quantities of data from disparate sources to construct "an intimate picture of the subject's life that he expects no one to have."[311] For DAS in particular, there can be no doubt about its capacity to facilitate broad programs of indiscriminate surveil-

306. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (discussing how court-imposed limitations on warrants for physical searches ensure the constitutionality of those searches).

307. 132 S. Ct. at 948.

308. *See generally id.*

309. *Id.* at 954.

310. For example, sections 331 to 334, and 903 of the FAA Modernization and Reform Act of 2012, H.R. 658, 112th Cong. (2nd Sess. 2012), dramatically expands access to, use of, and research into aerial drones in domestic airspace.

311. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010).

lance. As Mayor Bloomberg told reporters when unveiling the program:

> Investigators will have immediate access to information through live video feeds, and instantly see suspect arrest records, 911 calls associated with the suspect, related crimes occurring in the area and more . . . . Investigators can track where a car associated with a suspect is located, and where it has been in past days, weeks or months . . . .[312]

Although the Court has yet to consider the Fourth Amendment implications of data aggregation and data mining technologies, it has highlighted the privacy concerns at stake in other constitutional and statutory contexts. For example, in *United States Department of Justice v. Reporters Committee for Freedom of the Press*[313] the Supreme Court assessed the reach of Freedom of Information Act (FOIA) exemption 7(c), which prohibits federal disclosure of "records or information compiled for law enforcement purposes" that could "reasonably be expected to constitute an unwarranted invasion of personal privacy."[314] The Court held that the exemption prohibited disclosure of FBI "rap sheets" to the media even though these records are compiled entirely from information already available in public records.[315] In reaching that result, the Court focused on the expanding capacity of database technology to aggregate and store mass quantities of personal data.[316] The Court saw "a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[317] The privacy interest in criminal rap sheets was deemed "substantial" under FOIA because "in today's society the computer can accumulate and store information" to such an extent and degree that it violates a "privacy interest in maintaining the practical obscurity" of that information.[318] This, of course, was

312. Matt Williams, *New York City Shows New Law Enforcement Technology*, GOV'T TECH., Aug. 8, 2012, http://www.govtech.com/public-safety/New-York-City-Shows-New-Law-Enforcement-Technology.html.

313. 489 U.S. 749 (1989).

314. 5 U.S.C. 552(b)(7)(C).

315. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 767 (1989) (2012).

316. *Id.* at 770.

317. *Id.* at 764.

318. *Id.* at 780; *see also* Woodrow Hartzog & Frederic D. Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597745 (importing the

in 1989.[319] The technologies for both data gathering[320] and data storage[321] have increased in power on an exponential scale over the intervening years, measured now not in bytes or megabytes, but in zettabytes and yottabytes,[322] while costs have fallen past negligible.[323]

The political branches have also wrestled with the privacy consequences of data aggregation technologies. In 1973, the

notion of practical obscurity from *Reporters* to the private collection of online personal data).

319. *See generally* 489 U.S. 749 (1989).

320. Scott Shane, *Data Storage Could Expand Reach of Surveillance*, N.Y. TIMES: THE CAUCUS BLOG (Aug. 14, 2012, 5:50 PM), http://thecaucus.blogs.nytimes.com/2012/08/14/advances-in-data-storage-have-implications-for-government-surveillance/ (reporting that "the technology to capture and store such data is no longer a limiting factor [for the Data Awareness Program]"). By their nature, data aggregation systems take advantage of existing surveillance pathways, and therefore require very little additional costs. For example, the recently revealed program operated by the Federal Bureau of Investigation and the National Security Agency gathering metadata for all telephonic communications in the United States costs the government nothing because the data is gathered by telephone companies and passed to the National Security Agency under order of the Foreign Intelligence Surveillance Court. *See In re* Application of the FBI for an Order Requiring the Productino of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc., No. BR13-80, at 1 (FISA Ct., Apr. 25, 2013) (unpublished), *available at* http://www.theguardian.com/world/interactive/2013/jun/06/Verizon-telephone-data-court-order. So too, the much broader data collection efforts reported by James Bamford and described by whistleblower Edward Snowden providing government access to the contents of virtually every electronic communication that travels through the United States. *See* Glenn Greenwald, Ewen MacAskill, & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN, June 9, 2013, http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; *see also* Bamford, *The NSA is Building, supra* note 6.

321. *See* Shane, *supra* note 320 (reporting that "[t]he estimated cost of storing on gigabyte of digital data, adjusted for inflation to 2011 dollars, fell from $85,000 in 1984 to 5 cents in 2011"). In 2011, a report from the Brookings Institute estimated that it would cost the government 17 cents on a per capita basis to store all telephone conversations conducted in the United States, falling to 2 cents by 2015. JOHN VILLASENOR, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS, RECORDING EVERYTHING: DIGITAL STORAGE AS AN ENABLER OF AUTHORITARIAN GOVERNMENTS 4 (Dec. 14, 2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf. Although the estimated cost for constructing NSA's Cybersecurity Data Center at Camp Marshall in Utah is estimated at $2 billion, its storage capacity will be measured in zettabytes (10^{21} bytes) or yottabytes (10^{24} bytes), making it a bargain even by those projected 2015 cost standards. *See* Bamford, *The NSA is Building*, *supra* note 6.

322. *See* Bamford, *The NSA is Building*, *supra* note 6.

323. *See supra* notes 320–21 and accompanying text.

Secretary of the Department of Health, Education, and Welfare issued a report specifying the privacy concerns raised by computerized collections of personal data and offering a code of "fair information practices" that would provide procedural safeguards against the technology's inherent potential for abuse.[324] Embodying those fair information practices, the Privacy Act of 1974 (Privacy Act) prohibited federal agencies from maintaining secret systems of personal records[325] and from amassing personal information without a proper purpose.[326] Many information privacy laws also require opt-in consent before information can be gathered and shared. For example, the Children's Online Privacy Protection Act of 1998 (COPPA) essentially bans commercial websites directed at children under thirteen from collecting information directly from youths without a parent or guardian's verifiable knowledge and consent.[327] More recently, proposals for "Do Not Track" legislation would limit Internet companies from collecting consumers' web-browsing data to instances where the consumer agreed to such collection under an opt-in regime.[328]

324. REGAN, *supra* note 39, at 76.

325. *See* 5 U.S.C. § 552a (2006) (regulating federal government agencies' collection, use, and disclosure of personal information).

326. *See* 5 U.S.C. § 552a(e)(1) (agencies shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President"). The Privacy Act was passed out of concern over "the impact of computer data banks on individual privacy." H.R. Rep. No. 93-1416, at 7 (1974).

327. 15 U.S.C. §§ 6501–06 (2000). As Anita Allen explains, under COPPA, parents are "ascribed a powerful right to veto primary collection, primary use, secondary use, and even maintenance of data." ALLEN, *supra* note 92, at 178. In response to COPPA, social network sites like Facebook only permit users who are 13 and up; obtaining verifiable parental consent is both costly and risky if entities learn that parental consent is not valid, as the Federal Trade Commission has enforcement power over COPPA violations. *Id.* at 179–80 (discussing the FTC's enforcement actions for COPPA violations). Nonetheless, as social media scholar Danah Boyd and her colleagues have shown, parents routinely assist young children in lying to social network sites like Facebook so that their children can use those services, in some sense turning the purpose of the statute on its head. Danah Boyd et al., *Why Parents Help Their Children Lie to Facebook About Their Age: Unintended Consequences of the 'Children's Online Privacy Protection Act'*, FIRST MONDAY, Nov. 7, 2011, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075.

328. In 2011, several "Do Not Track" bills were proposed that would protect consumer information from being used without consent. Mark Hachman, *Do Not Track Legislation on the Move*, PC MAG., May 6, 2011, http://www.pcmag.com/article2/0,2817,2385045,00.asp.

These past efforts by the Court and the political branches to develop constraints on the deployment and use of data aggregation technologies provide useful models for accommodating Fourth Amendment interests implicated by technologies like DAS. When considering the options, it is critical to highlight the fact that some data aggregation technologies cannot adequately serve legitimate government interests if they can be deployed only in the context of discrete investigations and with the prior approval of a court. That is because systems like DAS are designed for early detection and to create an archived record of information that can be mined retrospectively.[329] To serve those purposes, these technologies need to be running all the time. If law enforcement agencies were required to develop probable cause before deploying a system like DAS, then these critical interests would not be served. On the other hand, these systems, by their very nature, engage in precisely the sort of broad and indiscriminate surveillance that is characteristic of a surveillance state, and therefore threaten reasonable expectations of quantitative privacy.[330] Where, then, are we to strike a reasonable balance between these competing interests?

Where data aggregation and mining technologies like DAS are concerned, we suspect that the best way to accommodate both law enforcement interests and interests in quantitative privacy is through negotiated agreements akin to consent decrees. Consent decrees are a common tool used by parties to cases challenging the constitutionality of law enforcement practices. For example, in *Handschu v. Special Services Division*,[331] the New York City Police Department entered into an agreement with civil rights advocates and labor organizations that limited investigations of purely political activity and indiscriminate photography at political gatherings. The terms of the agreement were enforced in the first instance by a special commission of the NYPD, which then answered to the United

329. *See* Rocco Parascandola & Tina Moore, *NYPD Unveils New $40 Million Super Computer System that Uses Data from Network of Cameras, License Plate Readers and Crime Reports*, N.Y. DAILY NEWS, Aug. 8, 2012, http://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135 (reporting how DAS may be mined).

330. *See* Bill Keller, *Living with the Surveillance State*, N.Y. TIMES, June 16, 2013, http://www.nytimes.com/2013/06/17/opinion/keller-living-with-the-surveillance-state.html (likening DAS to Orwell's "Big Brother" of 1984).

331. 605 F. Supp. 1384 (S.D.N.Y. 1985).

States District Court for the Southern District of New York.[332] The terms of the *Handschu* consent decree, and its enforcement structure, served a purpose similar to Odysseus's decision to bind himself to the mast of his ship so he could listen to the Sirens' song without running the risk that he would steer himself and his crew onto the Sirenum scopuli.[333] The consent decree allowed law enforcement to pursue legitimate criminal investigations that intersected with political activities within the bounds of rule-ordered supervision designed to minimize the risk that their investigations would indiscriminately infringe First Amendment freedoms. A similar approach holds significant promise for protecting Fourth Amendment rights against the indiscriminate use of data aggregation and mining technologies like DAS.

Once it is established that technologies like DAS implicate reasonable expectations of quantitative privacy, it will be incumbent upon law enforcement agencies to coordinate with citizens and interest groups to develop regulatory frameworks that strike a reasonable balance between competing interests.[334]

In most cases, these agreements will feature limits on the scope of data collection, retention, and use[335]—what Jon Elster might call "technological precommitments"[336]—implemented through design choices and administrative review structures.

332. *Id.* at 1389–90.

333. HOMER, THE ODYSSEY 276–77 (Robert Fagles trans., Penguin Books 1997). For more on the dynamics of precommitment and rationality, see JON ELSTER, ULYSSES AND THE SIRENS: STUDIES IN RATIONALITY AND IRRATIONALITY 36–47 (1979).

334. Although we do not endorse all of its recommendations, or necessarily regard them as sufficient, the Technology and Privacy Advisory Committee designated by then-Secretary of Defense Donald Rumsfeld in February 2003 to offer recommendations on how data aggregation systems incorporated into the defunct Total Awareness System might be deployed and used consistent with rights to privacy provides an example of the sort of joint effort we have in mind. *See generally* TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM (2004).

335. *See* TAPAC, *supra* note 83, at 41–42 (discussing the dangers associated with unlimited data retention and recommending government agencies and their agents "clearly specif[y] the purposes of data mining, carefully evaluat[e] the fitness and relevance of data for the intended purpose, leav[e] the data in place whenever possible, and implement[] systems for updating or discarding outdated information").

336. We refer here to Jon Elster's important work on reason, rationality, and constitutional constraint. *See generally* JON ELSTER, ULYSSES UNBOUND: STUDIES IN RATIONALITY, PRECOMMITMENT, AND CONSTRAINTS (2000).

Both these negotiated arrangements and their application in particular cases would, of course, be subject to court review for Fourth Amendment sufficiency. Here again, experience can help to guide us.

In at least some cases where law enforcement has deployed data aggregation technologies, there have been some efforts to effect restraints on collection, retention, and use of data. For example, the FBI has for some time been using proprietary software called EP2P that allows agents to identify the source of images containing child pornography that are distributed through peer-to-peer networks.[337] Although the technology behind EP2P could be used to search all files lodged on a suspect's computer—or all files on all computers linked to a peer-to-peer network—the software is designed such that agents can only access folders that are designated as "shared."[338] New York officials report that images aggregated by DAS will be destroyed after thirty days unless they are part of an active investigation.[339] As another example, the company Palantir, which develops data analysis software for security and law enforcement applications,[340] incorporates use controls and audit logs into their products that limit human access while providing a record of who has queried a database, when, and why.[341] By using meta-database management systems capable of searching across many discrete "federated" databases, data can also be kept in place rather than being aggregated into massive repositories, thereby limiting both the scope of surveillance and the potential for abuse by inserting access and use controls both across and between databases and search agents.[342] We are not sug-

337. *See* United States v. Budziak, 697 F.3d 1105, 1107–08 (9th Cir. 2012) (describing the Federal Bureau of Investigation's "EP2P" software); United States v. Chiaradio, 684 F.3d 265, 271–72 (1st Cir. 2012) (differentiating the Federal Bureau of Investigation's EP2P software from the commercially available program "LimeWire"); United States v. Gorski, 71 M.J. 729, 731–33 (Army Ct. Crim. App. 2012) (describing use of a "peer-to-peer" (P2P) network to share and distribute files).

338. *Budziak*, 697 F.3d at 1108.

339. *See* Shane, *supra* note 320; *see also* TAPAC, *supra* note 83, at 41–42 (recommending that data aggregation programs "implement[] systems for updating or discarding outdated information").

340. *What We Do*, PALANTIR, http://www.palantir.com/what-we-do/ (last visited Oct. 15, 2013).

341. *What We Believe*, PALANTIR, http://www.palantir.com/what-we-believe/#civilLiberties (last visited Oct. 15, 2013).

342. *See* TAPAC, *supra* note 83, at 41 (recommending leaving the data in place whenever possible); PALANTIR TECHNOLOGIES INC., A CORE COMMITMENT: PROTECTING PRIVACY AND CIVIL LIBERTIES, 3 (2012) (describing feder-

gesting that these efforts are necessary or sufficient to mark a reasonable balance between the interests of law enforcement and those of quantitative privacy, but, in our view, they signal important steps in that direction and provide a useful set of examples and experiences that can help ground conversations about the terms of deployment and use that should govern other data aggregation technologies.

By contrast, the data aggregation programs operated by the FBI and NSA, which gather metadata for every telephonic communication in the United States[343] and aim to capture and store the contents of all electronic communications in massive servers housed in places like Camp Marshall in Utah,[344] seem dramatically overbroad and utterly disconnected from anything beyond the most general and diffuse of government interests.[345] They are, in short, the very model of broad and indiscriminate surveillance. As a consequence, the court orders issued against companies like Verizon constitute a contemporary form of the general warrants targeted by the Fourth Amendment at its inception.[346] Faced with public criticism, advocates for these surveillance programs have offered two major lines of defense.

First, proponents have argued that the Foreign Intelligence Surveillance Act (FISA) sanctions these programs and that members of Congress have been briefed on a regular basis without objecting.[347] Of course, the raison d'être of constitutions

ated database architecture and how it can be used to enhance privacy protections).

343. *See In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [redacted], No. BR 13-80 (F.I.S.C., Apr. 25, 2013) *available at* http://apps.washingtonpost.com/g/page/politics/government-documents-related-to-nsa-collection-of-telephone-metadata-records/351/ (ordering the disclosure of "all call detail records or "telephony metadata" created by [Verizon] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.").

344. *See* Bamford, *The NSA is Building*, *supra* note 6.

345. Given this massive and unreasonable disconnect, we are particularly gratified to see a bi-partisan group of legislators organizing around an effort—so far unsuccessful—to constrain NSA data gathering to targets who are actually suspected of wrongdoing. *See* Jonathan Weisman, *Momentum Builds Against N.S.A. Surveillance*, N.Y. TIMES, July 28, 2013, *available at* http://www.nytimes.com/2013/07/29/us/politics/momentum-builds-against-nsa-surveillance.html?pagewanted=all&_r=0.

346. *See* Otis, *supra* note 217. Not only are these FISA orders overbroad, parallel revelations about the extensive use of independent contractors present us with a contemporary instance of the delegation powers that our founders regarded as odious features of writs of assistance and other general warrants.

347. Press Release, U.S. House of Representative Permanent Select Comm.

is to set limits on what the political branches can do through legislation or policy.[348] In the shadow of their experiences with writs of assistance and the Townshend Act, our late-eighteenth century forebears adopted the Fourth Amendment as a bar on legislative attempts to license general warrants or otherwise to sanction policies of broad and indiscriminate search using the political process.[349] Thus, to the extent that the FISA licenses new forms of general warrants and programs of broad and indiscriminate surveillance, it is unconstitutional and the review and approval of some members of congress is irrelevant.[350]

Second, defenders of these large-scale data aggregation programs have argued that access to the resulting databases is limited by internal agency rules and policies.[351] A redacted de-

on Intelligence, Joint Statement by House Intelligence Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger (June 6, 2013), *available at* http://intelligence.house.gov/press-release/joint-statement-house-intelligence-chairman-mike-rogers-and-ranking-member-ca-dutch ("The collection described with yesterday's disclosure of a purported court order is consistent with the Foreign Intelligence Surveillance Act (FISA) as passed by Congress, executed by the Executive Branch, and approved by a Federal Court . . . . When these authorities are used, they are governed by court-approved processes and procedures. Moreover, the use of these authorities is reviewed and approved by federal judges every 90 days. Additionally, the Committee routinely reviews all FISA activities."). Their assertions have since been backed up by the declassification of agency letters sent by the Department of Justice's Office of Legislative Affairs to members of Congress. *See* Letter from Ronald Weich, Assistant Attorney General, U.S. Dep't of Justice, to Sivestre Reyes, Chairman, Permanent Select Comm. on Intelligence, U.S. House of Representatives (Dec. 14, 2009), *available at* http://apps.washingtonpost.com/g/page/politics/government-documents-related-to-nsa-collection-of-telephone-metadata-records/351/; Letter from Ronald Weich, Assistant Attorney Gen., U.S. Dep't of Justice, to Diane Feinstein, Chairman, & Saxby Chambliss, Vice Chairman, Select Comm. on Intelligence, U.S. Senate (Feb. 2, 2011), *available at* http://apps.washingtonpost.com/g/page/politics/government-documents-related-to-nsa-collection-of-telephone-metadata-records/351/.

348. JON ELSTER, ULYSSES AND THE SIRENS: STUDIES IN RATIONALITY AND IRRATIONALITY 36–47 (1979); David Gray, *Why Justice Scalia Should Be a Constitutional Comparativist . . . Sometimes*, 59 STAN. L. REV. 1249, 1266 (2007); Antonin Scalia, *Common-Law Courts in a Civil-Law System: The Role of the United States Federal Courts in Interpreting the Constitution and Laws*, *in* A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 3, 40–41 (Amy Gutmann ed., 1997).

349. Davies, *supra* note 42, at 578–81, 657–60, 663–64, 668 ("[The framers] thought the important issue, and the only potential threat to the right to be secure, was whether *general* warrants could be authorized by *legislation*.").

350. It would also cut against the grain of FISA itself, which was passed to constrain the NSA's demonstrated tendency to pursue ever more expansive surveillance.

351. Jeffrey Rosen, *Control Your Spooks*, NEW REPUBLIC, July 15, 2013, at 22 (describing James Clapper's claims that rules attached to the original data

scription of these minimization procedures contained in a Foreign Intelligence Surveillance Court (FISC) order was declassified by the NSA in advance of congressional hearings on July 31, 2013.[352] Although much is still unknown, we see both promise and disappointment in these procedures as they have so far been described. Let us first consider the good.

There are, broadly, three issues at stake when evaluating the deployment and use of data aggregation technologies: collection, access, and retention. As described, the minimization procedures do constrain access and also set limits on retention. According to the order, all metadata that is collected must be housed in "secure networks under NSA's control."[353] Only "authorized personnel who have received appropriate and adequate training"[354] have access, and they are limited to conducting manual or automated "chain[ed] queries" using "seed" terms approved in advance by a select group of senior intelligence officials or the FISC.[355] Users are also subject to authentication and their queries audited.[356] Senior intelligence and Department of Justice officials are required to meet and review compliance with these procedures and to report their findings to the FISC on a regular basis.[357] Finally, the order provides that all metadata that is collected will be destroyed no later than five years after collection.[358] Many of these constraints on access and retention no doubt hold promise as executives, legislatures, and courts strive to effect the reasonable balance between law enforcement interests and citizen privacy demanded by the Fourth Amendment. Many questions remain, of course, among them details about what constitutes "appropriate and adequate training," auditing procedures, and court oversight.

Now, let us consider the bad. The most significant problem

aggregation warrants issued by the Foreign Intelligence Surveillance Court in support of these programs set limits on access).

352. *See In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [redacted], No. BR 13-80 (F.I.S.C., Apr. 25, 2013), *available at* http://apps.washingtonpost.com/g/page/politics/government-documents-related-to-nsa-collection-of-telephone-metadata-records/351/.

353. *Id.* at 4.

354. *Id.* at 5. The Order provides an exception to this rule for "technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA . . . ." *Id.* at 5 n.3.

355. *Id.* at 6–11.

356. *Id.* at 12–14.

357. *Id.* at 15–18.

358. *Id.* at 14.

with the data aggregation programs described in these leaked documents is the indiscriminate breadth of collection. No matter how strict, access rules and limits on retention simply cannot render "reasonable" data collection programs that are fatally broad and indiscriminate. These programs clearly cross that threshold. It is impossible to imagine that any but the smallest mote of data gathered is relevant to anti-terrorism efforts. In fact, senior government officials have admitted as much.[359] Furthermore, the vast majority of cases cited by supporters of the programs' success seem to involve queries based on evidence gathered through traditional law enforcement means.[360] In these circumstances, more narrowly tailored, case specific, data gathering would have done just as well, and certainly would have reflected a more reasonable balance between law enforcement interests and citizen privacy.[361] Also important is the fact that none of these procedures has been subject to the crucible of adversarial challenge. That is because the NSA has kept the programs secret while simultaneously arguing that nobody has standing to bring a challenge unless they can prove that they have been monitored, which is impossible because the program is kept secret.[362] We therefore do not know, and cannot

359. Robert Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Remarks at the Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction (June 26, 2013) (transcript on file with authors) ("Each determination of a reasonable suspicion under this program must be documented and approved, and only a small portion of the data that is collected is ever actually reviewed, because the vast majority of that data is never going to be responsive to one of these terrorism-related queries.").

360. *See id.* ("The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations.").

361. *See* Charlie Savage, *Surveillance Programs Defended as Officials Cite Thwarted Attacks*, N.Y. TIMES, June 19, 2013, at A18 ("Representative Adam B. Schiff, Democrat of California, pressed General Alexander to explain why the F.B.I. could not simply get the relevant logs of calls linked to a suspicious number without keeping a database of all domestic calls. General Alexander said he was open to discussing doing it that way, but added, '[t]he concern is speed in crisis.'").

362. *See* Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013). An action filed by the ACLU challenging the NSA's gathering of telephonic metadata appears to have cleared this hurdle, but was only able to do so because an NSA contractor leaked top-secret documents. *See* Complaint at 6, Am. Civil Liberties Union v. Clapper, No. 13 Civ. 3994 (S.D.N.Y. filed June 11, 2013), *available at* http://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf. The Electronic Privacy Information Center and the Electronic Frontier Foundation have since filed actions challenging the NSA's massive data gathering on statutory and First Amendment grounds. *See In re* Elec. Privacy Info. Ctr., No. 13 (*petition*

really evaluate, the adequacy of these measures to the task of constraining law enforcement discretion.[363] It is hard to imagine that those who read and wrote the text of the Fourth Amendment would have thought that it allowed the government not only to conduct searches pursuant to general warrants, but to do so in secret. Thus, there is simply no other way to view these programs than as constitutionally unreasonable; and the authority granted to them by the FISC as general warrants.

* * *

Although this Article is the first to advance a coherent, doctrinally grounded proposal for regulating general surveillance and data aggregation technologies like DAS, there is good reason to think that law enforcement agencies will be receptive. The NYPD has committed itself to some checks on information retention and sharing coordinated by DAS—including the thirty-day retention policy mentioned above—in its "Public Security Privacy Guidelines."[364] The policy sets limits on how long certain data will be stored and pledges to share information only with private "stakeholders" who have signed memoranda of understanding.[365] It further claims that "[d]igital watermarking or an equivalent technique will be used to create an immutable audit log of where and when data is accessed."[366] Linking these technological pre-commitments to supervising administrative bodies—such as the special commission designated in *Handschu*—that are empowered to monitor use and to impose civil and administrative penalties in cases of abuse would provide further assurances that programs like DAS are serving legitimate law enforcement interests while still protecting reasonable expectations in quantitative privacy.[367] Courts must

for cert. filed July 8, 2013), *available at* https://epic.org/EPIC-FISC-Mandamus-Petition.pdf (challenging the program on statutory grounds); Complaint at 13, First Unitarian Church of L.A. v. Nat'l Sec. Agency, No. CV 13-3287 (N.D.C.A., filed July 16, 2013), *available at* https://www.eff.org/file/37386#page/28/mode/2up (challenging the program on First Amendment grounds).

363. *Cf.* Davies, *supra* note 42, at 556, 578–81, 655–57 (arguing that the founders' primary concern when adopting the Fourth Amendment was to limit the licensing of unconstrained discretion, specifically through the use of general warrants).

364. *Public Security Privacy Guidelines*, N.Y.C. POLICE DEP'T, (Apr. 2, 2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf.

365. *Id.*at 2.

366. *Id.* at 7.

367. *See* Handschu v. Special Servs. Div., 605 F. Supp. 1384, 1402 (S.D.N.Y. 1985).

retain final authority to review the decisions and conduct of any such administrative panels, of course; but active, responsive, and thoughtful internal review procedures will make court intervention less necessary and therefore less frequent. The NSA, FBI, and other federal agencies involved in collecting telephonic metadata have also instituted controls. Although they are inadequate given the sheer breadth and scale of the data that is being collected, they might well render constitutional a more targeted program. For the present, however, we are heartened by the effort, which we see as an important positive signal in the context of ongoing efforts to understand and accommodate Fourth Amendment protections of quantitative privacy.

D. THE TECHNOLOGY-CENTERED APPROACH AND HUMAN SURVEILLANCE

There is a heated debate after *Jones* over the implications of quantitative privacy for many traditional law enforcement methods. For example, Orin Kerr has wondered whether "visual surveillance [should] be subject to [mosaic analysis]."[368] Justice Scalia expressed similar concerns in his majority opinion in *Jones*.[369] Adding weight to their fears, Christopher Slobogin, a mosaic theory advocate, has argued that human surveillance should be subject to the same Fourth Amendment regulations as GPS-enabled tracking.[370]

Our technology-centered approach would not implicate human surveillance and other traditional investigative techniques. As Justice Alito observed in *Jones*, "[human] surveillance for any extended period of time [is] difficult and costly and therefore rarely undertaken."[371] Because human surveillance is incapable of sustaining the sort of broad and indiscriminate surveillance that is characteristic of a surveillance state, it would not be subject to Fourth Amendment regulation under our technology-centered approach.[372] This result would not

368. Kerr, *supra* note 33, at 335.

369. United States v. Jones, 132 S.Ct. 945, 953–54 (2012).

370. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 757 (1993).

371. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

372. This marks a significant point of departure between us and most other contributors to the post-*Jones* debate, including Christopher Slobogin. *See, e.g.*, Slobogin, *supra* note 53, at 25 (proposing legislative limitations on human

change even if law enforcement assembled a detailed mosaic documenting the activities of an individual suspect using multiple traditional law enforcement methods.[373] Why? Because these mosaics, by virtue of how they are assembled, simply do not raise the specter of a surveillance state, and therefore do not trigger Fourth Amendment interests in quantitative privacy.[374]

* * *

Although necessarily brief, the foregoing provides a general account of how a technology-centered approach to quantitative privacy would work in practice, and how it would apply to different kinds of surveillance technologies and methods, including drones, GPS-enabled tracking, DAS, the NSA's telephonic and electronic surveillance program, and human surveillance. This goes part way to answering the demands of skeptics on and off the Court for a workable approach to Fourth Amendment cases after *Jones*.[375] We continue the journey in Part IV by explaining how our technology-centered approach answers or moots many of the most persistent objections that have been raised by quantitative privacy skeptics.

IV. SOME CONCERNS ABOUT QUANTITATIVE PRIVACY IN PRACTICE

Proposals to extend Fourth Amendment protections to cover reasonable expectations of quantitative privacy have been met with considerable resistance.[376] This Part addresses some of the most salient criticisms.[377] As our discussion shows, these challenges mainly target the "mosaic" theory of quantitative privacy. Among the many advantages of our technology-centered approach is that it avoids many of these concerns.

surveillance conducted for periods longer than twenty minutes).

373. Thus, our technology-based approach also answers Orin Kerr's concerns about how quantitative privacy would apply to bodies of information aggregated by different law enforcement groups or agencies. *See* Kerr, *supr*a note 33, at 347.

374. We are in debt to James Grimmelmann for pressing us to clarity on this point.

375. *See, e.g.*, *Jones*, 132 S. Ct. at 953–54; Kerr, *supra* note 33, at 343–50. We discuss how our technology-centered approach would provide a clear road forward on the facts of *Jones* below. *See infra* notes 410–29 and accompanying text.

376. *See, e.g.*, *Jones*, 132 S. Ct. at 953–54; Kerr, *supra* note 33, at 343–50.

377. For an extended analysis of objections to the mosaic theory, see Gray & Citron, *supra* note 53, at 398–11.

A. THE TECHNOLOGY-CENTERED APPROACH RESOLVES PRACTICAL CHALLENGES

Critics contend that recognizing a quantitative dimension to Fourth Amendment privacy creates thorny practical challenges.[378] Among the most nettlesome is drawing lines between quanta of information that implicate reasonable expectations of privacy and those that do not.[379] Justice Scalia levels this charge in *Jones*, pointing out that Justice Alito's concurring opinion does not explain why short-term monitoring is acceptable but "a 4-week investigation is 'surely' too long."[380] Orin Kerr has echoed Justice Scalia's concerns.[381] Kerr has also expressed reservations about how to parse mosaics that are aggregated using a variety of techniques and technologies.[382]

Although these line-drawing challenges may have some traction against a mosaic theory of quantitative privacy,[383] they have no bite at all against our technology-centered proposal. Whereas a case-by-case approach to quantitative privacy requires courts to evaluate the Fourth Amendment interests implicated by individual mosaics, a technology-centered approach interrogates the potential for abuse *inherent* in a given surveillance technology. As new surveillance technologies become available, courts will need to determine whether those technologies have the capacity to facilitate the sorts of broad programs of indiscriminate surveillance that raise constitutional concerns about a surveillance state. If a particular technology does not raise these concerns, then the Fourth Amendment simply does not apply. If it does, then the government will only be allowed to use that technology when it can meet the demands of Fourth

378. *See, e.g.*, *Jones*, 132 S.Ct. at 953-54; Kerr, *supra* note 33, at 343–50.

379. *See* Slobogin, *supra* note 53, at 6, 17.

380. *Jones*, 132 S. Ct. at 954. We discuss *Knotts* at greater depth below. *See infra* notes 410–29 and accompanying text.

381. Kerr, *supra* note 33, at 333 ("[H]ow long must the tool be used before the relevant mosaic is created?").

382. *Id*. at 335–36.

383. Of course, worries about line drawing are by no means unique to quantitative privacy. The Fourth Amendment's center of gravity is reasonableness. *See* Akhil Amar, *Terry and the Fourth Amendment First Principles*, 72 ST. JOHN'S L. REV. 1097, 1101 (1998). Assessments of reasonableness are inherently prone to spectrums and nuances, and seldom are amenable to bright line rules and dramatic contrasts. Despite these difficulties, the Court has yet to abandon a constitutional protection simply because it is challenging to enforce. Rather, the Court leaves it to the lower courts to mush through the "factbound morass of 'reasonableness.'" Scott v. Harris, 550 U.S. 372, 383 (2007).

Amendment reasonableness.[384] To be sure, assessments of reasonableness—by balancing the interests of law enforcement and citizens—present their own challenges; but they are both familiar and inherent to Fourth Amendment itself.[385] They are also downstream struggles. Under our approach, the upstream question of whether use of a technology constitutes a search at all is answered *as a general matter* for that technology rather than on a case-by-case basis.[386]

The results of an upstream search inquiry should not change merely because a surveillance technology is commonplace. In holding that thermal detection technology should be subject to Fourth Amendment regulation in *Kyllo v. United States*, Justice Scalia contemplated the possibility that the result in that case might have been different if that technology was in "general public use."[387] The implication is that, if a technology is in general public use, then it is unreasonable, as a descriptive matter, for anyone to expect that they are not being observed with that technology by fellow citizens, and therefore also unreasonable, as a normative matter, to expect that law enforcement officers should be constrained by the Fourth Amendment.[388] This is technological determinism run amok. As Justice Scalia argued in *Kyllo*, "the power of technology to shrink the realm of guaranteed privacy" *must* be limited lest we "permit police technology to erode the privacy guaranteed by the Fourth Amendment."[389] The alternative is to require that citizens "retir[e] to the cellar, cloaking all the windows with thick caulking, turning off the lights and remaining absolutely quiet."[390] When faced with this alternative, "we must ask what we will have saved if we cede significant ground to a bunker mode of existence, retaining only that sliver of privacy that we

384. *See, e.g.*, Katz v. United States, 398 U.S. 347, 350 (1967).

385. *See id.* at 354.

386. For the same reason, our technology-centered approach avoids problems relating to human-collected surveillance mosaics collected via multiple investigative tools and methods. For reasons described above, human surveillance is not a technology that implicates quantitative privacy. *See supra* notes 369–74.

387. Kyllo v. United States, 533 U.S. 27, 40 (2001).

388. *Cf.* United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy . . . .").

389. *Kyllo,* 533 U.S. at 34; *see also* Amsterdam, *supra* note 210, at 384 ("Fortunately, neither *Katz* nor the fourth amendment asks what we expect of government. They tell us what we should demand of government.").

390. Amsterdam, *supra* note 210, at 402.

cannot envision a madman exploiting."[391] To paraphrase one learned member of the bench, we "simply cannot imagine that the drafters of the Fourth Amendment dictated such dark and cloistered lives for citizens."[392]

Our technology-centered approach also helps to clarify or resolve other practical challenges leveled against quantitative privacy. For example, in *Jones*, Justice Alito argues that, "longer term GPS monitoring in investigations *of most offenses* impinges on expectations of privacy."[393] This suggests that whether an investigative technology constitutes a Fourth Amendment search relates in part to the seriousness of the crime under investigation. As Justice Scalia rightly points out for the majority, "[t]here is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated."[394] As our technology-centered approach makes clear, however, there is simply no argumentative clash here.

Justice Scalia is surely right that the nature of the offense being investigated has no relevance to the upstream question of whether law enforcement conduct constitutes a "search." Citizens do not possess greater expectations of privacy in less serious crimes.[395] The seriousness of an offense is, however, highly relevant to the downstream question of whether a search is "reasonable."[396] As we pointed out in Part III, assessing Fourth Amendment reasonableness is a matter of balancing citizen interests with those of law enforcement. Law enforcement naturally has a weightier interest in detecting and prosecuting more serious crimes than it does for minor offenses.[397] When weigh-

391. Hutchins, *supra* note 135, at 464.

392. Palmieri v. Lynch, 392 F.3d 73, 97 (2d Cir. 2004) (Straub, J., dissenting); *see also* Amsterdam, *supra* note 210, at 402 ("This much withdrawal is not required in order to claim the benefit of the amendment because, if it were, the amendment's benefit would be too stingy to preserve the kind of open society to which we are committed and in which the amendment is supposed to function"); Crocker, *supra* note 204, at 369 ("[P]lacing pressure on persons to return to their individual 'private' worlds to seek refuge from government searches and surveillance diminishes the public sphere's security.").

393. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (emphasis added).

394. *Id.* at 954.

395. *Id.*

396. Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 4 (2011) ("A key intuitive component of reasonableness is the seriousness of the crime investigated."); *cf.* 18 U.S.C. § 2516(1)(a)–(s) (2012) (limiting use of wiretapping technology to investigations of enumerated offenses).

397. *See* Bellin, *supra* note 396, at 9 ("The public's interest in any search or seizure surely depends to some degree on the seriousness of the crime under

ing the reasonableness of a search, the seriousness of the offense being investigated is therefore relevant.[398] Likewise, courts can, and should, consider the seriousness of the offense being investigated as a factor when determining whether law enforcement officers acted reasonably during a search or seizure.[399] Thus, a court would be far more likely to grant a warrant for GPS-enabled tracking for a month if probable cause exists to believe both that the target is directing a large drug conspiracy and that the tracking will produce additional important evidence, as was in fact the case in *Jones*, but less likely to grant a similar warrant for a person suspected of perpetrating occasional minor speeding offenses.

Critics might grant us these points, but argue that our technology-centered approach comes with its own baggage. For example, a skeptic might argue that focusing on the technology begets its own line-drawing problems.[400] Specifically, they

investigation."); Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1598 (2010) (reporting that public opinion polls rate investigations of serious crimes as less intrusive than investigations of minor crimes); William J. Stuntz, *Commentary, O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 870, 875 (2001) ("A large factor in government need—perhaps the largest—is the crime the government is investigating . . . the worst crimes are the most important ones to solve, the ones worth paying the largest price in intrusions on citizens' liberty and privacy.").

398. *See* New Jersey v. T.L.O., 469 U.S. 325, 380 (1985) (Stevens, J., concurring and dissenting in part) ("The logic of distinguishing between minor and serious offenses in evaluating the reasonableness of school searches is almost too clear for argument."); Welsh v. Wisconsin, 466 U.S. 740, 750 (1984) ("Our hesitation in finding exigent circumstances, especially when warrantless arrests in the home are at issue, is particularly appropriate when the underlying offense for which there is probable cause to arrest is relatively minor."); McDonald v. United States, 335 U.S. 451, 459 (1948) (Jackson, J., concurring) ("Whether there is reasonable necessity for a search without waiting to obtain a warrant certainly depends somewhat upon the gravity of the offense thought to be in progress as well as the hazards of the method of attempting to reach it."); United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984) ("But maybe in dealing with *so* intrusive a technique as television surveillance, other methods of control as well, such as banning the technique outright from use in the home in connection with minor crimes, will be required, in order to strike a proper balance between public safety and personal privacy."); Christopher Slobogin, *The World Without the Fourth Amendment*, 39 UCLA L. REV. 1, 68–75 (1991).

399. *See* Tennessee v. Garner, 471 U.S. 1, 11 (1985) ("A police officer may not seize an unarmed, nondangerous suspect by shooting him dead."); Cipes v. Graham, 386 F. Supp. 2d 34, 41 (D. Conn. 2005) (citing the fact that plaintiff was only suspected of a misdemeanor offense as relevant to determining whether a nighttime raid of his house was "reasonable").

400. We are in debt to Richard Myers and others who have pressed us on

might argue that DAS and drones represent easy examples of technologies that raise quantitative privacy concerns, but that courts inevitably will confront technologies whose Fourth Amendment status is not as clear. These are not new problems for Fourth Amendment law, of course.[401] To the contrary, they are endemic to the reasonableness inquiry that lies at the heart of contemporary Fourth Amendment doctrine.[402] We therefore accept the inevitability of close cases. In doing so, however, we emphasize that the systemic burden of close cases will be much lighter under a technology-centered approach than they would be under a mosaic theory. That is because, whether it is a close call or not, once the Fourth Amendment status of a technology has been established, the threshold question of whether use of that technology constitutes a Fourth Amendment search does not need to be litigated in every case where the technology is used. By contrast, under a mosaic approach, whether a particular aggregation of information constitutes a search is a question that must be litigated de novo in every case because, like snowflakes, every mosaic will necessarily be unique.[403] We are also confident that the factors for evaluating the surveillance threat posed by a particular technology, such as scale, scope, and cost, are likely to be fewer and easier to apply with greater predictability than the many variables that would inform a mosaic analysis, where the idiosyncratic dispositions of judges likely would hold more than the usual sway.[404]

Critics of our technology-centered approach might also argue that law enforcement officers and agencies acting in their strategic modes will simply avoid Fourth Amendment regulation by making minor changes to regulated surveillance technologies in an ongoing game of "technological whack-a-mole."[405] Here again, these sorts of strategic games are not without precedent. For example, the advent of designer drugs has allowed

this point.

401. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 474–75 (1971) (finding no surprise and little weight in "the unstated proposition that when a line is drawn there is often not a great deal of difference between situations closest to it on either side").

402. *Id.*

403. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 953–54 (2012); Kerr, *supra* note 33, at 343–50.

404. *E.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001); *see also* Freiwald, *supra* note 41, at 5.

405. We owe this wonderful turn of phrase to Max Mishkin of Yale's Information Society Project.

manufacturers to simply change the chemical formulation of their products to avoid criminal liability—at least until the law catches up.[406] Similar games are played in the patent world.[407] The solution in these contexts is often to focus on function rather than precise chemical structure.[408] That same approach holds considerable promise in the present context to block attempts by law enforcement circumnavigate Fourth Amendment regulations.[409]

This discussion does not exhaust all of the practical challenges that proposals to defend reasonable interests in quantitative privacy must face. It nevertheless provides good grounds for believing that they can be met, and that our technology-centered approach offers a far better alternative than proposals for case-by-case methods based on the mosaic theory.

B. THE TECHNOLOGY-CENTERED APPROACH AND THE PUBLIC OBSERVATION DOCTRINE

Another potential bar to judicial recognition of quantitative privacy is stare decisis and particularly *United States v. Knotts*.[410] In *Knotts*, the Court held that using a beeper device to track a suspect's car on public streets did not constitute a "search" because the suspect lacked a reasonable expectation of privacy in his public movements.[411] The parallel between *Knotts* and *Jones* is obvious. In both cases, law enforcement officers used a passive signaling device attached to a car.[412] In both cas-

406. *See generally* Bertha K. Madras, *Designer Drugs: An Escalating Public Health Challenge*, 206 J. GLOBAL DRUG POL'Y & PRAC. 1 (2012), *available at* http://www.dfaf.org/webinar/files/designer_drugs.pdf.

407. *Cf.* Citron & Pasqual, *supra* note 22, at 1486 (exploring how fusion centers can engage in regulatory arbitrage by moving data mining to a jurisdiction with less restrictive privacy laws); Pamela Samuelson, *Intellectual Property Arbitrage: How Foreign Rules Can Affect Domestic Protections*, 71 U. CHI. L. REV. 223, 238 (2004) (discussing shifting of activity to jurisdictions with less regulatory restriction).

408. *See generally* Graver Tank & Mfg. Co. v. Linde Air Prods., Inc., 339 U.S. 605, 607–08 (1950).

409. This is precisely the approach adopted by Switzerland in revisions to its privacy laws. *See* Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, B.U. J. SCI. & TECH. L. (forthcoming 2013) (on file with authors) (describing how Swiss privacy laws are designed to accommodate changes in technology without requiring constant amendment to the codes themselves).

410. 460 U.S. 276 (1983).

411. *Id.* at 281.

412. *Id.* at 278; United States v. Jones, 132 S. Ct. 945, 948 (2012).

es, the devices revealed only movements on public streets.[413] In both cases, those movements were exposed to public view.[414] Given these parallels, *Knotts* would seem to control in cases like *Jones*, thus barring Fourth Amendment review of GPS-enabled tracking, drones, or data aggregation systems, so long as the technology is only used to monitor movements in public.[415] Should the Court eventually adopt the views expressed by the *Jones* concurrences, it therefore seems obliged to overrule *Knotts*.

Our technology-centered approach avoids this entanglement with stare decisis by providing easy grounds for distinguishing *Knotts* from cases that involve GPS-enabled tracking or other advanced surveillance technology like aerial drones.[416] The beeper technology used in *Knotts* was simply incapable of broad and indiscriminate surveillance. It could only provide directional information, not a suspect's precise location.[417] To be of any use at all, the beepers used in *Knotts* needed to be in close proximity to a dedicated radio receiver.[418] Because no stable network of these receivers existed, officers had to follow the beepers, and hence the suspects, to track them.[419] This beeper technology was thus little more than an adjunct to traditional human surveillance and therefore labored under the same practical limitations.[420] That is why the *Knotts* Court ultimately held that the beeper technology used in that case "raise[d] no constitutional issues which visual surveillance would not also raise."[421]

The GPS-enabled tracking technology used in *Jones* and other technologies that threaten quantitative privacy are materially different.[422] They therefore implicate markedly "different

413. *Knotts*, 460 U.S. at 281; *Jones*, 132 S. Ct. at 948.

414. *Id.*

415. It would have to be public movements. *See* United States v. Karo, 468 U.S. 705, 713–14 (1984).

416. *See Jones*, 132 S. Ct. at 954.

417. With a stable network of receivers, officers might have been able to triangulate Knotts's position. Cellular phone providers presently can locate subscribers' phones using this same technique. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 683 (2011).

418. *Knotts*, 460 U.S. at 278.

419. *Id.*

420. *See Jones*, 132 S. Ct. at 964 n.10 (Alito, J., concurring).

421. *Knotts*, 460 U.S. at 285.

422. *See* Hutchins, *supra* note 135, at 414–21.

constitutional principles."[423] GPS-enabled technology provides second-by-second location data. Like drones, GPS is precise, highly scalable, and increasingly inexpensive.[424] Due to the nearly ubiquitous reach of satellite networks, GPS technology has extensive range and can locate devices within a range of several feet.[425] Unlike the beeper technology in *Knotts*, GPS-enabled tracking devices gather locational data without any need for human beings to "tail" targets.[426] Officers can monitor the movements of a GPS-enabled device from anywhere at any time or automate their work by allowing a computer to do the monitoring for them.[427] GPS networks can also cheaply track millions of devices, and algorithms can search unlimited hours of locational data for significant patterns.[428] Thus, granting law enforcement unfettered access to GPS-enabled tracking technology raises the specter of a surveillance state.[429] The constitutional distinction between *Knotts* and *Jones* is therefore not that officers exercised restraint in their use of technology in *Knotts*, but, rather, that the technology used in *Knotts* came with inherent constraints that limited its ability to facilitate broad programs of indiscriminate surveillance. The GPS technology used in *Jones* suffers no such limitations.

C. THE TECHNOLOGY-CENTERED APPROACH AND THE STATE AGENCY REQUIREMENT

In her concurring opinion in *Jones*, Justice Sotomayor suggests that recognizing a constitutional dimension to quantitative privacy might require "reconsider[ing] the premise that an individual has no reasonable expectation of privacy in infor-

423. *Knotts*, 460 U.S. at 284.

424. Farhad Manjoo, *Keeping Loved Ones on the Grid*, N.Y. TIMES, Oct. 25, 2012, at D1.

425. *See* Hutchins, *supra* note 135, at 418–20.

426. Michael Ferraresi, *GPS Makes Police Officers' Job Easier, Safer*, ARIZ. REPUBLIC, Oct. 7, 2005, http://www.azcentral.com/community/scottsdale/articles/1007sr-technology07Z8.html.

427. Carrie Johnson and Steve Inskeep, *GPS Devices Do the Work of Law Enforcement*, NAT'L PUB. RADIO (Oct. 27, 2010), http://www.npr.org/templates/story/story.php?storyId=130851849.

428. *See* Slobogin, *supra* note 53, at 2; Erik Eckholm, *Private Snoops Find GPS Trail Legal to Follow*, N.Y. TIMES, Jan. 29, 2012, at A1 (reporting that sales of GPS-enabled tracking devices surpass 100,000 a year and are rising); Ben Hubbard, *Police Turn to Secret Weapon: GPS Device*, WASH. POST, Aug. 13, 2008, at A1, *available at* http://www.washingtonpost.com/wpdyn/content/article/2008/08/12/AR2008081203275.html?nav=rss_metro/va.

429. Hutchins, *supra* note 135, at 421.

mation voluntarily disclosed to third parties."[430] Her concern seems to be that substantive Fourth Amendment interests threatened by broad and indiscriminate surveillance are no less at stake when information is gathered through private actors than when it is gathered or aggregated by the government directly.[431] To the extent that she is right, it would appear that private data collections assembled by service providers, such as Verizon, or data brokers, like Acxiom, provide a wide avenue by which the government could circumnavigate efforts to protect Fourth Amendment interests in quantitative privacy. Although compelling, we doubt that dramatic doctrinal changes are necessary to meet Justice Sotomayor's concerns. To explain why, let us first briefly elaborate two lines of Fourth Amendment doctrine that intersect with Justice Sotomayor's concerns: the state action requirement and the third-party doctrine.

The Information Privacy Law Project has long been concerned with privacy violations that citizens perpetrate against each other in their private roles. From the start, it has relied on, and responded to, Samuel Warren and Louis Brandeis's seminal 1890 article, which focused on violations of "the right 'to be let alone'"[432] perpetrated by the press to satisfy the "prurient taste[s]" of its readership.[433] In that spirit, scholars have drawn attention to the privacy implications of developing technology when wielded by private entities.[434] Various efforts have

430. Jones v. United States, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also* Crocker, *supra* note 204 (arguing for a modification of the third-party doctrine).

431. *Jones*, 132 S. Ct. at 957.

432. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting THOMAS MCINTYRE COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888)).

433. *Id*. at 194–96. ("When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance. Easy of comprehension, appealing to that weak side of human nature which is never wholly cast down by the misfortunes and frailties of our neighbors, no one can be surprised that it usurps the place of interest in brains capable of other things. Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence."). Although credit is due to Alan Westin for creating the field of information privacy law, we regard Warren and Brandeis's seminal 1890 article as the first contribution to what has since come to be the Information Privacy Law Project. *See* Danielle Citron, *In Honor of Alan Westin: Privacy Trailblazer, Seer, and Changemaker*, CONCURRING OPS. (Feb. 24, 2013), http://www.concurringopinions.com/archives/2013/02/in-honor-of-alan-westin-privacy-trailblazer-seer-and-changemaker.html.

434. *See, e.g.*, SOLOVE, DIGITAL PERSON, *supra* note 87, at 5–15.

also been made to develop legislative and common law protections.[435] No matter how intrusive, however, these private infringements are beyond the reach of the Fourth Amendment. That is because, as the Court has long held, "the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative."[436]

An important consequence of this state agency requirement is that the Fourth Amendment is not implicated if the fruits of a private search are passed along to government agents.[437] That result does not change if the private search is unlawful.[438] The state agency requirement therefore appears to have serious consequences for efforts to secure Fourth Amendment interests in quantitative privacy. Faced with Fourth Amendment constraints, law enforcement might simply contract with a private drone operator or private data aggregator to benefit indirectly from technology that it cannot use directly.[439] Fortunately, existing doctrine closes this loophole.

The Fourth Amendment is implicated not only when government employees engage directly in a search, but also when a private party acts as an "agent or instrument of the [g]overnment."[440] Whether a private party is considered an agent of the government for Fourth Amendment purposes "turns on the degree of the Government's participation in the private party's activities."[441] This is "a question that can only be resolved in light of all the circumstances."[442] That the "[g]overnment has not compelled a private party to perform a search does not, by itself, establish that the search is a private one."[443] For a private party to be considered a state actor, the government does not need to be "the moving force of the

435. Among these is the American Law Institute's recent commitment to draft a Restatement of Information Privacy Principles under the leadership of Paul Schwartz and Dan Solove as the Reporters. One of us (Citron) is part of the small group of scholars, judges, advocates, and industry leaders who will be helping to draft them.

436. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989); Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

437. Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

438. *Burdeau*, 256 U.S. at 475.

439. Robert O'Harrow, Jr., *Centers Tap Into Private Databases*, WASH. POST, Apr. 2, 2008, http://articles.washingtonpost.com/2008-04-02/news/36868484_1_fusion-centers-databases-credit-reports.

440. *Skinner*, 489 U.S. at 614–15.

441. *Id.* (citations omitted).

442. *Id.* at 614–15 (citations and internal quotation marks omitted).

443. *Id.* at 615.

search."[444] The private search does not even need to be done for the purpose of advancing a law enforcement purpose.[445] All that is necessary is some "clear indic[ation] of the Government's encouragement, endorsement, and participation."[446] This threshold will usually be met where a private entity is directed or incentivized by the government, where the private entity reasonably believes that it is acting on state authority or direction, or where a government agent knows or has reason to know that the private entity is acting to advance state goals.[447] The direct participation of a government official in an otherwise private search would certainly be enough.[448] A contractual relationship or specific statutory authorization would also suffice if it demonstrated a governmental "desire to share the fruits" of a private search.[449]

We suspect that, in most cases where the government's benefitting from private surveillance or leveraging private data reservoirs would raise the specter of a surveillance state, there will also be sufficient evidence of government encouragement, sponsorship, or participation to bring the private entity's activities under Fourth Amendment review. DAS, a joint Microsoft and NYPD project, is illustrative. The NYPD could not avoid Fourth Amendment regulation of DAS by simply outsourcing DAS and its operation to a private contractor because that contractor would be acting as an agent of the NYPD.[450] The result would not be different if DAS was developed and deployed by a private company which then sold its services to the NYPD. To be of much benefit, the technology would need access to information controlled by the government.[451] The private company would also depend, in part or in whole, on income from government sources.[452] At the least, government would have an

444. *Cf.* Lustig v. United States, 338 U.S. 74, 78 (1949).

445. *Cf. id.*

446. *Skinner*, 489 U.S. at 615–16.

447. *Id.*

448. *See* Byars v. United States, 273 U.S. 28 (1927).

449. *Skinner*, 489 U.S. at 615–16.

450. *See* Ferguson v. City of Charleston, 532 U.S. 67, 72, 82 (2001).

451. We might say the same about Google's involvement in building Virtual Alabama for Alabama's Department of Homeland Security. *See* McKenna, *supra* note 21. Under its license for the technology, Alabama can add data from all available sources. Virtual Alabama is also encouraging contributions from private entities in exchange for access to the system. If Google operated Virtual Alabama and provided analysis to Alabama's DHS, then Google should surely be considered a state agent with respect to those activities.

452. TORIN MONAHAN, SURVEILLANCE IN THE TIME OF INSECURITY 47

abiding interest in the data, manifested by repeated requests for information. These facts would certainly be sufficient to show state agency. By contrast, if no such facts existed, then there would be no specter of a surveillance state.[453] On this account, Verizon and other telecommunication companies that have been subject to FISA orders *demanding* the production of metadata for all domestic and international telephone communications on a rolling and continuous basis for many years running are acting as state agents—though perhaps unwilling—when they collect and aggregate that data for the NSA and FBI.[454]

D. THE TECHNOLOGY-CENTERED APPROACH AND THE THIRD-PARTY DOCTRINE

In addition to end-runs around the Fourth Amendment via the state-agency requirement, Justice Sotomayor's concerns in *Jones* implicate the third-party doctrine, which holds that the Fourth Amendment is not violated if the government obtains information from a third party that an investigative target voluntarily shared with that third party.[455] Applying this doctrine, the Court has held that there is no Fourth Amendment violation if a bank shares customers' financial records with law en-

(2010) (describing trade shows devoted to private security contractors selling their wares to government agencies).

453. Following Warren and Brandeis, we might nevertheless like to set limits on what these purely private entities do, but that would be a task for the political branches or the common law of torts, not the Fourth Amendment.

454. *Cf.* Ted Ullyot, *Facebook Releases Data, Including all National Security Requests*, FACEBOOK NEWSROOM (June 14, 2013), http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests ("For the six months ending December 31, 2012, the total number of user-data requests Facebook received from any and all government entities in the U.S. (including local, state, and federal, and including criminal and national security-related requests)—was between 9,000 and 10,000. These requests run the gamut—from things like a local sheriff trying to find a missing child, to a federal marshal tracking a fugitive, to a police department investigating an assault, to a national security official investigating a terrorist threat. The total number of Facebook user accounts for which data was requested pursuant to the entirety of those 9–10 thousand requests was between 18,000 and 19,000 accounts."). The same may well be true of companies such as Facebook, Google, and Apple who are ordered to participate in the NSA's Prism program. Because the details of this program, including the technology used, the scope of aggregation, and the level of government access, have so far remained secret, it is at this point premature to even speculate.

455. *See* United States v. Miller, 425 U.S. 435, 442–43 (1976); Hoffa v. United States, 385 U.S. 293, 302 (1966).

forcement,[456] or if a telephone company discloses records of phone calls customers have made or received.[457] Although the Court has not been entirely clear on the underlying justification for the third-party doctrine, the most coherent is that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government" by lawful means.[458] As the Court has pointed out, that risk does not diminish "even if the information is revealed [to the third party] on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[459]

Law enforcement investigations frequently employ cooperating witnesses, confidential informants, and even undercover police officers.[460] No matter how surprised or dismayed the target of such investigative strategies may be, the third-party doc-

456. *Miller*, 425 U.S. at 442–43; *see also* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 69 (1974) (holding that statute requiring banks to keep copies of customers' checks does not implicate the Fourth Amendment). Congress responded to *Miller* and *Schultz* by passing the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–22, which provides bank customers some privacy regarding their records held by banks and other financial institutions and stipulates procedures whereby federal agencies can gain access to those records.

457. Smith v. Maryland, 442 U.S. 735, 744 (1979) (explaining that a person who uses the phone "assume[s] the risk that the [telephone] company would reveal to police the numbers he dialed"). *See* SOLOVE, DIGITAL PERSON, *supra* note 87, at 205. ("The Pen Register Act attempt[ed] to fill the void left by *Smith v. Maryland* by requiring a court order to use a pen register or trap and trace device. Whereas a pen register records the [tele]phone numbers a person dials from [a] home, a trap and trace device creates a list of the telephone numbers of incoming calls."); *see also* 18 U.S.C. § 3121(a) (2006).

458. *Miller*, 425 U.S. at 443 (quoting United States v. White, 401 U.S. 745, 751–52 (1971)). In *Miller* and other cases in the line, the Court has also suggested that citizens retain no reasonable expectation of privacy at all in information shared with third parties. *See Smith* 442 U.S. at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *Miller*, 425 U.S. at 442. This seems to be how Justice Sotomayor reads the rule as well. *See* Jones v. United States, 132 S. Ct. 945, 957 (2012) (describing the third-party doctrine as "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"). This, of course, is far too broad, and if taken at face value would mean that *Katz* itself was wrongly decided insofar as the words intercepted by the government's "electronic ear" in that case had been voluntarily shared by Katz with a third-party conversant. We therefore assume that the third-party doctrine relies on some version of the narrower misplaced trust rationale.

459. *Miller*, 425 U.S. at 443.

460. *See, e.g.*, Lewis v. United States, 385 U.S. 206 (1966) (undercover agents); Hoffa v. United States, 385 U.S. 293 (1966) (confidential informant); Lopez v. United States, 373 U.S. 427 (1963) (cooperating witness).

trine holds that he simply has no Fourth Amendment complaint if those with whom he shared information in confidence decide to violate that trust, whether voluntarily, under force of subpoena, or by threat of contempt.[461] In the age of data aggregation, the stakes for privacy implicated by this third-party doctrine have grown dramatically.[462] Vast reservoirs of our private data are gathered by or otherwise reside in the hands of private entities.[463] GPS chips in telephones, cars, or computers share a steady stream of information about our movements with companies that provide services associated with these devices.[464] Internet Service Providers and search engines log where we go and what we do online.[465] Credit card companies and other vendors record and analyze our shopping habits.[466] In all of these cases, the information is freely shared with a person or entity so they can provide a service or convenience.[467] Under the third-party doctrine, we have no Fourth Amendment complaint if recipients share that information with the government.[468]

The implications for Fourth Amendment interests in quantitative privacy are obvious. What the government cannot col-

461. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 53 (1974).

462. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 248–49 (2007).

463. *See id*.; Slobogin, *supra* note 53, at 7.

464. Christopher Williams, *Police Use TomTom Data to Target Speed Traps*, TELEGRAPH, Apr. 28, 2011, *available at* http://www.telegraph.co.uk/technology/news/8480195/Police-use-TomTom-data-to-target-speed-traps.html.

465. Danielle Keats Citron, *The Privacy Implications of Deep Packet Inspection*, *in* OFFICE OF PRIVACY COMMISSIONER OF CANADA, DEEP PACKET INSPECTION: A COLLECTION OF ESSAYS FROM INDUSTRY EXPERTS, *available at* http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/.

466. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0.

467. *See* Jones v. United States, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy . . . .").

468. *See* United States v. Miller, 425 U.S. 435, 440–43 (1976) (holding that bank customers cannot raise a Fourth Amendment bar against government subpoena for bank records documenting their transactions because banks and their customers are parties to the underlying transactions, and customers must share information about those transactions with their banks in order for the banks to perform their roles); *cf. Jones*, 132 S. Ct. at 962 ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.") (Alito, J., concurring).

lect or aggregate directly, it can simply get from third parties with whom the information has been shared.[469] If the government lacks legal authority to install and monitor a GPS-enabled tracking device, then it can get the same information by securing locational data from OnStar, Lojac, a cellular phone provider, or any number of "apps" that gather and use locational information as part of their services. This is not an abstract concern. As of this writing, a case is working its way through the New York courts involving a subpoena served on Twitter by the Manhattan District Attorney's office seeking, among other things, locational data embedded in a user's postings.[470] Both Twitter and the user moved to quash the subpoena, but the Supreme Court denied both motions, relying in part on the third-party doctrine.[471]

As discussed in the Introduction, recently leaked documents reveal that every telecommunications company doing business in the United States has been subject to rolling orders issued by the Foreign Intelligence Surveillance Court since at least 2006 demanding the production of "all call detail records or 'telephony metadata'" for every domestic and international telephone call.[472] This metadata, when checked against other data, enable the discovery of callers' identities, locations, social contacts, and group affiliations including the political, religious, and social, both mainstream and fringe.[473] This is exactly the sort of detailed personal information that concerned the concurring justices in *Jones*.[474]

Whether implemented directly or indirectly through private actors, the effects of the surveillance state on projects of personal development and democratic culture are likely to be the same. In fact, they might be worse. Much of the hope and promise of networked technologies is that they expand the horizons of our personal explorations and associations while providing diverse forums for civil society engagements that would otherwise be impractical or impossible. That potential

469. Citron & Pasquale, *supra* note 22, at 1451.

470. People v. Harris, 945 N.Y.S.2d 505 (N.Y. Crim. Ct. 2012).

471. *Id*. at 507; Megan Guess, *Twitter Hands over Sealed Occupy Wall Street Protestor's Tweets*, ARS TECHNICA (Sept. 14, 2012), http://arstechnica.com/tech-policy/2012/09/twitter-hands-over-occupy-wall-street-protesters-tweets/.

472. FISA, *supra* note 2, at 2.

473. Roberts & Ackerman, *supra* note 3.

474. United States v. Jones 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring); *Id.* at 954–56 (Sotomayor, J., concurring).

would be severely compromised if we knew the government was or well might be watching everything we read, write, or do in the digital world.[475] The problem remains if, rather than watching directly, the government could simply accomplish its surveillance through third-party service providers. Of course, we could avoid being watched by simply withdrawing from these worlds; but, as one of us has argued elsewhere, this is a Hobson's choice, at least insofar as liberty and democratic participation are valuable and constitutionally protected social goods.[476]

Among the strengths of our technology-centered approach is that it can guard against these concerns without needing to effect dramatic changes to the third-party doctrine. To see why, it is necessary to say a bit more about the doctrine's conceptual structure. Although it overstates matters a bit to suggest that the third-party doctrine relies on "the premise that an individual has no reasonable expectations of privacy in information voluntarily disclosed to third parties,"[477] there is no doubt that the third-party doctrine has the same basic conceptual foundation as the public observation doctrine. Although the universe of persons with whom we share information about our movements in public is, at least in theory, larger than the universe of people with whom we share, say, information about our financial transactions, in both cases the act of sharing affects our reasonable expectations of privacy. As we have argued at length in this Article, however, surveillance technology may raise Fourth Amendment issues independent of our expectations of privacy in the discrete bits of information gathered by that technology. The result would not be any different just because the information is shared with a small group of people rather than the public at large. In either case, Fourth Amendment interests in quantitative privacy will be implicated if the technology used to gather the information raises the specter of a surveillance state by facilitating programs of broad, indiscriminate surveillance.

475. Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance's Privacy Harms: A Reply to Professor Neil Richards*, 126 HARV. L. REV. 1934 (2013).

476. Danielle Keats Citron, Hate 3.0: A Civil Rights Agenda to Combat Online Harassment (forthcoming 2014) (on file with autor); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 105 (2009).

477. *Jones*, S. Ct. at 957; *see also* Crocker, *supra* note 204 (arguing for a modification of the third-party doctrine).

Let us return to the example of DAS. The System's core function is to aggregate data from diverse sources, including traffic cameras, toll cameras, surveillance cameras, cell phone providers, GPS-based services, credit card companies, banks, and internet service providers. Although most of the data coming into DAS when considered discretely would not implicate reasonable expectations of privacy under either the third-party doctrine or the public observation doctrine, DAS nevertheless epitomizes the surveillance state because its very function is to facilitate a program of broad and indiscriminate surveillance. Its deployment and use should therefore be subject to Fourth Amendment regulation.

The result should not be different if the aggregator is a private entity acting as a state-agent rather than the government itself. Take as an example the data broker Acxiom, which uses proprietary technology to collect and mine a mind-boggling array of data about people from various public and third-party sources, including social network activity, property records, public-health data, criminal justice sources, car rentals, credit reports, postal and shipping records, utility bills, gaming, insurance claims, divorce records, browsing habits compiled by behavioral advertisers, and purchasing histories gathered using vendor discount cards, among other sources.[478] Chris Hoofnagle has dubbed data brokers like Acxiom as "Big Brother's Little Helpers" because government and law enforcement are among their most important clients.[479] With this level of government engagement, there is little doubt that Acxiom and its kin are state agents, at least when conducting business for or on behalf of the government.[480] Thus, Acxiom's activities should be subject to Fourth Amendment review when it is acting as an arm of the government.

None of this requires abandoning or modifying the third-party doctrine. It remains true that we have no Fourth

478. *See* Danielle Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPS. (June 19, 2012, 5:08 PM), http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html.

479. Hoofnagle, *supra* note 24, at 595.

480. So too are the many telephone and electronic communication companies that provide government agencies with user information so frequently that they have standing price lists describing what they charge to deploy their search and aggregation technologies for government purposes. *See* Andy Greenberg, *These are the Prices AT&T, Verizon, and Sprint Charge for Cellphone Wiretaps*, FORBES, Apr. 3, 2012, http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps/.

Amendment complaint if a third party with whom we share information gathers that information in traditional ways and passes it along to the government. There is also no Fourth Amendment issue just because investigators collect a detailed mosaic of personal information on a suspect. Rather, it is the means that matter. Thus, the Fourth Amendment would not be implicated if a third party used pen registers or similar technology to gather evidence for the government because these technologies are too limited to facilitate the sort of broad and indiscriminate surveillance characteristic of a surveillance state.[481] By contrast, the data aggregation technologies deployed by Verizon and other telecommunications companies to provide the FBI and the NSA with "telephony metadata" for all calls "between the United States and abroad" and all calls "wholly within the United States, including local telephone calls"[482] implicate "different constitutional principles."[483] By virtue of their scale and scope, these data aggregation capacities epitomize a surveillance state when put at the service of government.[484] Verizon's use of these technologies at the behest government agencies should therefore be subject to Fourth Amendment regulation.

481. This is not to suggest that these more limited technologies do not raise serious privacy issues. Rather, the point is that those privacy interests must be addressed by the political branches through legislation or executive order rather than by the Fourth Amendment. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 905, 931–39 (2008) (discussing state privacy legislation); SOLOVE, DIGITAL PERSON, *supra* note 87, at 202–08 (discussing various legislative regimes regulating government access to third-party records that were passed in response to the Supreme Court's refusal to find the Fourth Amendment applicable). Congress did of course step in to limit the use of pen registers. *See* 18 U.S.C. § 3121(a) (2012). Although critics can certainly argue that the political branches' records are hardly perfect on these scores, we prefer constitutional humility and doctrinal parsimony to Fourth Amendment overreach.

482. FISA, *supra* note 2, at 2.

483. United States v. Knotts, 460 U.S. 276, 284 (1983).

484. As Jameel Jaffer put the point:

> From a civil liberties perspective, the program could hardly be any more alarming. It's a program in which some untold number of innocent people have been put under the constant surveillance of government agents. It is beyond Orwellian, and it provides further evidence of the extent to which basic democratic rights are being surrendered in secret to the demands of unaccountable intelligence agencies.

Roberts & Ackerman, *supra* note 3.

CONCLUSION

Recognizing a constitutional interest in quantitative privacy buttresses Fourth Amendment defenses against a surveillance state. Until now, practical limitations inherent to many investigative techniques, cultural constraints on mutual surveillance, and existing Fourth Amendment doctrines have provided a virtual guarantee that traditional investigative techniques would not produce the kind of broad and indiscriminate monitoring that raises the specter of a surveillance state. There simply are not enough police officers to follow all of us all of the time. As a society, we have stalwartly resisted the temptations of mutual surveillance that sustained many totalitarian states. Fourth Amendment doctrine has also preserved an archipelago of safe spaces and activities beyond the gaze of government agents. As a consequence, we have until now sustained a fairly stable balance between government power and private citizenship that allows us to pursue projects of self-development free from fear that the government is watching.[485]

Recent technological developments, such as the NSA's broad and indiscriminate data collection, aggregation, and retention programs, New York's Domain Awareness System, aerial drones, and GPS-enabled tracking devices threaten to alter this balance. By their nature, these technologies make possible the monitoring of everyone all the time. As consequence, granting the government unfettered access to these technologies opens the door to a surveillance state and the tyranny it entails. It is therefore at the point of unfettered access to those technologies that the Fourth Amendment should intervene. As we have argued here, this technology-centered approach to quantitative privacy holds great promise in our continuing efforts to strike a reasonable balance between the competing interests of law enforcement and citizen privacy while preserving the critical service of the Fourth Amendment as a bulwark against the rise of a surveillance state.

485. *See generally* Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).