2014

Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance

Olivier Sylvain
Fordham University School of Law, sylvain@fordham.edu

FAILING EXPECTATIONS: FOURTH AMENDMENT DOCTRINE IN THE ERA OF TOTAL SURVEILLANCE

Olivier Sylvain[*]

INTRODUCTION

Entrepreneurs are eagerly developing techniques to monetize the massive amount of data that course through the networked information economy every day. Major telecommunications companies and Internet companies in particular are designing services and applications that lure users into volunteering as much personal information as possible. These firms use data to market services or trade with third parties.

Users, meanwhile, are of two minds about these data-sharing arrangements. On the one hand, polls suggest that users have serious concerns.[1] On the other hand, the sheer pace of growth of the consumer market for networked services and devices strongly suggests that they are comfortable enough to share personal information about their identities, locations, and preferences. Users do not appear to be deterred by shifting privacy policies and long-worded terms of service that detail how much of their information will be traded.[2] To the contrary, if consumer demand is any measure of interest, users appear to welcome innovations that track

* Associate Professor, Fordham University School of Law. I am grateful to the *Wake Forest Law Review* for hosting the symposium on digital privacy. I also am indebted to Danielle Citron, Susan Freiwald, Sonia Katyal, Andrew Kent, Christopher Hoofnagle, Olatunde Johnson, Joel Reidenberg, Neil Richards, Zephyr Teachout, and Alexander Tsesis for helpful comments about this Essay. All remaining errors are mine.

1. *See* Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RES. INTERNET PROJECT 2 (Sept. 5, 2013), http://pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf ("Most internet users would like to be anonymous online at least occasionally, but many think it is not possible to be completely anonymous online."); *see also* Jan Lauren Boyles et al., *Privacy and Data Management on Mobile Devices*, PEW RES. INTERNET PROJECT 2 (Sept. 5, 2012), http://pewinternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf ("More than half of app users have uninstalled or decided to not install an app due to concerns about personal information.").

2. *See, e.g.*, Vindu Goel & Edward Wyatt, *Facebook Privacy Change Is Subject of F.T.C. Inquiry*, N.Y. TIMES, Sept. 12, 2013, at B1; Claire Cain Miller & Vindu Goel, *Google to Sell Users' Endorsements*, N.Y. TIMES, Oct. 12, 2013, at B1.

and even predict their tastes for new products and services.[3] Users appear to expect that their personal data is the proverbial grist for today's networked information economy.

In this way, the networked information economy has done wonders for government surveillance as well. It is no longer a secret today that federal, state, and local officials use the massive stores of available data to paint a "mosaic" of users' past and current behaviors.[4] This potential for total government surveillance has opened the door to a whole new era that is evocative of the dystopic portrayals in popular books and films like *1984* and *Minority Report*. Every moment that a user is connected to the network has become an opportunity to be surveilled by law enforcement and national security agencies.[5] The sense of being watched all the time could chill users' willingness to speak their minds and associate with others in ways that are evocative of totalitarianism.

In this way, the large-scale law enforcement practice of collecting and sorting data is just one aspect of the "total surveillance" characteristic of the whole networked information economy.[6] Again, in spite of polls that suggest consumer unease about government surveillance, users nevertheless expect to give their personal information as the presumptive price to pay for being fully connected.

But there is one important difference. Commercial behavioral tracking and profiling is not held to as high a standard as government surveillance. Governments are limited by the warrant requirement under the Fourth Amendment; police officials cannot search someone without a particularized showing to a court that an investigating officer has probable cause to believe that some specific criminal activity is afoot.[7] In the event law enforcement officials do not obtain a warrant, courts make two related inquiries to

3. *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013) (describing how trends on social media websites can be used in this way). This paradox in consumer expectations is not new. Users were conflicted in the decades before the Court decided *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967), on how much they trusted law enforcement officials—that is, assuming they even gave state surveillance any thought. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 10–11 (2004) (discussing the paradox in consumer perceptions about surveillance in the decades before *Katz*). This confusion remains today. *Id.* at 27.

4. *Cf.* United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

5. *See, e.g.*, Charlie Savage, *C.I.A. Is Said to Pay AT&T for Call Data*, N.Y. TIMES, Nov. 7, 2013, at A1 (reporting that the C.I.A. paid AT&T for call data for surveillance purposes).

6. I owe the "total surveillance" term to Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935–36 (2013).

7. *See* U.S. CONST. amend. IV; *Katz*, 389 U.S. at 357.

determine whether law enforcement engaged in a search within the meaning of the Fourth Amendment: first, courts ask whether the target had a reasonable expectation of privacy at the time the police obtained the materials and, second, courts ask whether this expectation is one that society is prepared to recognize as legitimate.[8] This two-step standard has been the foundation of federal regulation of law enforcement surveillance since the late 1960s.[9]

To complicate matters, courts have also distinguished between government surveillance of communications content on the one hand and the monitoring of transactional information about communications on the other.[10] The first category covers the information that parties to a communication explicitly convey to each other. These communications could include, for example, conversations about a criminal conspiracy or a terrorist plot.[11] Communications content is direct evidence of specific motivations about imminent conduct.[12] The second category covers transactional information about the communication, including the times, places, phone numbers, and addresses. These data are indispensable features of any given communication; service providers must have transactional data about senders and addressees in order to administer the communication.[13]

The distinction between the two—content and transactional data—is significant because the warrant requirement does not apply to the second.[14] Courts have presumed that users consent to the public disclosure of transactional data when they volunteer them to their service providers.[15] The third-party doctrine presumes that,

8. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

9. *See, e.g.*, Graham B. Smith, Comment, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L. REV. 481, 485 (2001) (describing the federal laws enacted in response to the decision in Katz).

10. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741–46 (1979); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008), *overruled on different grounds by* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

11. *See, e.g.*, *Katz*, 389 U.S. at 354 (explaining how government agents did not begin their surveillance of the targets in that case until their investigation "had established a strong probability" that the telephone was used for criminal purposes); Berger v. New York, 388 U.S. 41, 45 (1967) (discussing how eavesdropping uncovered that plaintiff was "a go-between" in a conspiracy to issue liquor licenses).

12. *See, e.g.*, Osborn v. United States, 385 U.S. 323, 325–27 (1966) (finding that the contents of a taped conversation were highly probative in determining whether petitioner knowingly attempted to obstruct justice).

13. *See Smith*, 442 U.S. at 742–43.

14. *Id.* at 745–46.

15. *Id.* at 743.

when users share it with third-party service providers, they convey an expectation that the information is not private. Users do not have that expectation for the content of the communication.[16]

This Essay takes up and critiques the contemporary doctrine by posing two sets of related questions. First, what are we to do when noncontent information may reveal as much, if not more, intimate information about users than the content of communications do? That is, what if noncontent data reveal detailed information about favorite locations, periodic habits and dealings, and associations? Second, should we continue to allow service providers to trade noncontent transactional user data with governments without restriction when users volunteer those data for the sole purpose of obtaining the specific underlying service? Does it matter that, in the aggregate, transactional data expose behavioral patterns that users do not fully appreciate about themselves when they volunteer them to their service providers?

I argue here that today's reasonable expectation test and the third-party doctrine have little to nothing to offer by way of privacy protection if users today are at least conflicted about whether transactional noncontent data should be shared with third parties, including law enforcement officials. This uncertainty about how to define public expectation as a descriptive matter, I argue, has compelled courts to defer to legislatures to find out what public expectation ought to be as a matter of law. Courts and others presume that legislatures are far better than courts at defining public expectations about emergent technologies.[17] Legislatures, courts posit, are designed to receive all manner of evidence about public expectations and, subsequently, articulate their findings and conclusions in statutes. Elected officials, after all, must be true to their constituents' desires if they are to stay in office.

Courts, meanwhile, are by design isolated from electoral politics. It is in this vein that even they seem to agree that there is only so much they can say about public expectations of privacy in the context of emergent surveillance techniques.[18] Courts do not have at their disposal any articulated process in Fourth Amendment

16. *See Katz*, 389 U.S. at 353.

17. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06, 855 (2004) (arguing that legislatures, rather than courts, should determine search-and-seizure rules when technology is in flux); *see also* Richards, *supra* note 6, at 1958 ("Professor Orin Kerr is correct when he argues that federal statutory law has advantages over the Fourth Amendment in guarding against surveillance in the digital age. Not only is statutory law easier to change, but it also can be applied to bind both government and nongovernment actors." (internal citation omitted)).

18. *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring) (arguing that the legislature may be best suited to deal with privacy concerns stemming from new forms of technology).

doctrine to discover public expectation as a matter of course. Public expectation is more like a legislative fact, far better suited to discovery and deliberation in legislatures.[19]

I argue here that the reasonable expectation standard is particularly flawed if it has the effect of encouraging judges to seek guidance from legislatures on constitutional norms and principles. Judicial review is the vital antimajoritarian check against excessive government intrusions on individual liberty under our constitutional scheme. This is a responsibility that courts cannot pass off to the political branches when, as is the case today, most people expect that the cost of network connection is total surveillance.

Court-administered privacy law doctrine accordingly must change if the protection against "unreasonable searches and seizures" is to have any positive legal meaning. The current court-created doctrine will not be able to keep up if it compels judges to measure public expectation. It is time for courts to reassert their positive duty to say what privacy law is.

I. TOTAL SURVEILLANCE

A. The New Normal

The vast majority of people in the United States today take affirmative steps to keep their online behavior private.[20] Most, however, also believe that these efforts only go so far.[21] They expect that, no matter their efforts, most of what they do online can be discovered.[22]

Indeed, despite their misgivings, participation and upload rates at the top social networking sites and applications continue to grow. For example, over 1.2 billion users log in to their Facebook accounts at least every month.[23] That is around one-third greater than the number of user accounts Facebook had just a year before.[24] Of these, about 700 million are active daily users.[25] These users upload an average of more than 350 million photos every day, with a huge fraction of these pictures coming from smartphone cameras.[26] Meanwhile, about 500 million people have active Twitter accounts

19. *Id.* at 964.

20. *See* Rainie et al., *supra* note 1; *see also* Boyles et al., *supra* note 1.

21. *See* Rainie et al., *supra* note 1, at 12 ("Most do not think it is possible to be completely anonymous online, though a healthy minority believe they can be totally hidden.").

22. *Id.*

23. Facebook, Inc., Quarterly Report (Form 10-Q) 24 (Nov. 1, 2013).

24. *See* Facebook, Inc., Quarterly Report (Form 10-Q) 20 (Oct. 24, 2012) (reporting the monthly active users at 1.01 billion as of Sept. 30, 2012).

25. *See* Facebook, Inc., Quarterly Report (Form 10-Q) 23 (Nov. 1, 2013).

26. Facebook, Inc., Annual Report (Form 10-K) 5 (Feb. 1, 2013); *see also Always Connected: How Smartphones and Social Keep Us Engaged*, IDC 6–7 (2013), https://fb-public.app.box.com/s/3iq5x6uwnqtq7ki4q8wk.

from which they post nearly fifty-eight million tweets and photos every day.[27] If these popular Internet-based applications are any indication of how willing users are to publicize their personal information, we can assume that, no matter how uneasy they may be about disclosing so much,[28] users are still willing to do it.

Facebook, Twitter, and most other Internet companies generally do not have misgivings about collecting users' personal information. To the contrary, they see personal user data as the currency of the networked information economy.[29] For them, it is to be "reused, repurposed and sold to other companies" for secondary uses that no one really anticipated when the data were first collected.[30] As we speak, these firms are developing creative new techniques for tracking users' online behavior.[31]

B. Collection, Aggregation, and Sharing

In short, user tracking involves the collection, storage, and analysis of user data.[32] Sites and applications administer user information in this way in order to provide a specific, ostensibly user-friendly service.[33] Consider Amazon, Zappos, or any retail website which, upon a user search, lists the items sought by a user but also makes recommendations about other items that might interest the user. Collection and analysis in this case is

27. Twitter, Inc., Registration Statement (Form S-1) 1 (Oct. 3, 2013) (reporting the monthly active users as 215 million, and 500 million tweets per day as of October 3, 2013).

28. *See Internet Freedom Group Splits from Tech Companies over Surveillance Concerns*, HILL (Oct. 10, 2013, 6:41 PM), http://thehill.com/blogs/hillicon-valley/technology/327831-internet-freedom-group-splits-from-tech-companies-over-surveillance-concerns.

29. *See, e.g.*, Claire Cain Miller & Somini Sengupta, *Selling Secrets of Phone Users to Advertisers*, N.Y. TIMES, Oct. 6, 2013, at 1 (discussing how companies like Google and Facebook are trying to find new ways to monetize their user bases by finding way to target them with specific ads); Danny Yadron, *Private-Data Firms Draw Fire of FTC*, WALL ST. J., May 8, 2013, at B2 (reporting on how tech companies selling personal data might violate federal privacy law).

30. Michiko Kakutani, *Watched by the Web: Surveillance Is Reborn*, N.Y. TIMES, June 11, 2013, at C1 (reviewing Viktor Mayer-Schönberger and Kenneth Cukier's book, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013)).

31. *See, e.g.*, *Several Top Websites Use Device Fingerprinting to Secretly Track Users*, PHYS.ORG (Oct. 10, 2013), http://phys.org/news/2013-10-websites-device-fingerprinting-secretly-track.html; Jennifer Valentino-DeVries, *How to Prevent Device Fingerprinting*, WALL ST. J. (Nov. 30, 2010, 11:32 PM), http://blogs.wsj.com/digits/2010/11/30/how-to-prevent-device-fingerprinting/.

32. *See, e.g.*, *Data Use Policy*, FACEBOOK (Nov. 15, 2013), https://www.facebook.com/full_data_use_policy (discussing how Facebook tracks, stores, and uses user data).

33. *Id.*

contemporaneous and generally incidental to providing the services or products for which users sign up or log in.

Service providers, sites, and applications also hold the data for business-related purposes related to the underlying service or for use at some future date for some presently unknown future purpose.[34] For example, a department store might use data about a user's purchases of a specific line of men's clothing to market a novel new male antiperspirant. Or, more pertinently, it might sell or trade that information to another company with an interest in knowing who is buying a certain kind of product.

As intrusive as total surveillance is, most users seem resigned to the fact that service providers and online applications share their personal information with third-party data aggregators.[35] These aggregators—social networking sites and Internet search companies, as well as large credit agencies and commercial data brokers—hold extraordinary amounts of information about users.[36] With so much data comes the awesome power to define users based on disparate bits of information. Data holders can be a user's most trusted guide in a foreign country. But they might also use the information to guide you to more expensive products or even to destroy your reputation and economic well-being.[37]

These firms, meanwhile, assume that the benefits of large-scale data aggregation and sorting far exceed any of the disadvantages. Google and Facebook have developed algorithms that analyze the finest details of users' online behavior and send targeted advertisements to those users based on that information.[38] Users do

34. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1124–25 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc). *See generally* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1323–24 (2000) (discussing how aggregating and analyzing user data stored at "data warehouses" can reveal patterns in user behavior).

35. *See, e.g.*, Hadley Malcolm, *Millennials Don't Worry About Online Privacy*, USA TODAY (Apr. 21, 2013, 8:45 AM), http://www.usatoday.com/story/money/business/2013/04/21/millennials-personal-info-online/2087989/ (discussing the millennial generation's willingness to post personal information about themselves on the Internet).

36. *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Aga of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 240 (2013).

37. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258 (2008); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1760 (2010) (discussing "database[s] of ruin"); *see also* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. (forthcoming 2014) (manuscript at 29), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703##.

38. *See* Katja de Vries, *Privacy, Due Process and the Computational Turn: A Parable and a First Analysis*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 44, 52 (Mireille Hildebrandt & Katja de Vries eds., 2013) (discussing "machine learning").

not seem particularly bothered by disclosures because they continue to acquire applications that know or predict their tastes before they even know what they want.[39]

C. Paradoxes in Expectation

Private companies are not the only entities that trade and share users' personal online information. Governments, too, are in the business of collecting and analyzing personal data, and sometimes purchasing them.[40] Their reasons, however, are different. Federal, state, and local agencies generally rely on the interests in national security, law enforcement, and public safety. Emergent surveillance technologies are perfectly suited to achieving these public ends.[41] Properly designed algorithms can help to search online data for possible wrongdoing and even anticipate lawlessness.[42]

What has emerged, then, is a government-industry partnership that, on the one hand, counts on users' demonstrable willingness to share personal information with data brokers and, on the other hand, furthers the government interest in public safety.[43] This is not a devious plan that was hatched in some dark, shadowy office on Capitol Hill or at Fort Meade, although it sometimes feels that way.[44] The Internet's early designers and proponents did not have total surveillance in mind. To the contrary, the early designers sought to avert centralized control, placing the intelligence of the network at the "ends" with users.

The Internet changed quite dramatically after Congress formally commercialized it in the mid-1990s.[45] Indeed, since then, total surveillance has become its defining characteristic. Today, the most popular service providers, sites, and applications have

39. *See generally* ELI PARISER, FILTER BUBBLE (2011) (discussing the dangers of this new era of personalization); Claire Cain Miller, *New Apps Know the Answer Before You Ask the Question*, N.Y. TIMES, July 30, 2013, at A1.

40. *See* Craig Timberg & Barton Gellman, *NSA Pays Firms Large Sums for Network Access*, WASH. POST, Aug. 30, 2013, at A1.

41. *See* Citron, *supra* note 37, at 1252–53.

42. *See* Martijn van Otterlo, *A Machine Learning View on Profiling*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY, *supra* note 38, 103, 103–07.

43. *See* Bruce Schneier, *The Public-Private Surveillance Partnership*, BLOOMBERG (July 31, 2013), http://www.bloomberg.com/news/2013-07-31/the-public-private-surveillance-partnership.html.

44. *See, e.g.*, Ryan Singel, *Whistle-Blower Outs NSA Spy Room*, WIRED (Apr. 7, 2006), http://www.wired.com/science/discoveries/news/2006/04/70619 (discussing secretive Bush-era eavesdropping).

45. *See Internet History*, CONNECTED: INTERNET ENCYCLOPEDIA, http://www.freesoft.org/CIE/Topics/57.htm (last visited Mar. 25, 2014) (discussing the commercialization of the Internet in the 1990s).

designed sophisticated techniques for aggregating and sharing as much data about each and every visitor as legally possible.[46]

And users have been complicit at every step, divulging all manners of information in order to receive the full benefits of the networked information economy. They volunteer their personal information to service providers and application developers and, whether they know it or not, allow those companies to monitor and trade this information with third parties.[47]

But users today are generally undecided about total surveillance when government agencies are involved. They want it both ways. On the one hand, they volunteer personal information to service providers and application developers.[48] Yet, users are also wary of sharing too much, especially when the government is involved.[49] They would like to be anonymous online, sometimes even as they also recognize that complete anonymity is impossible.[50]

This is the contemporary paradox of total surveillance today; people aspire to control what governments know about them, but they also believe that public exposure is inevitable, and perhaps even necessary, in a fully interconnected world.

II. EXPECTATION IN AN AGE OF TOTAL SURVEILLANCE

A. Reasonable Expectation

Total surveillance in liberal democracies substantially transforms the relationship between individuals and their government.[51] The "panoptic gaze" of constant government surveillance is arguably the most dangerous threat to personhood and citizenship. Total government surveillance in particular has

46. *See Several Top Websites Use Device Fingerprinting to Secretly Track Users*, *supra* note 31; Valentino-DeVries, *supra* note 31.

47. *See* Tene & Polonetsky, *supra* note 36; *see also* Rainie et al., *supra* note 1.

48. *See* Malcolm, *supra* note 35 (discussing this trend in the context of the Millennial generation).

49. *See* Jon Cohen & Dan Balz, *Poll: Privacy Concerns Rise After NSA Leaks*, WASH. POST (July 24, 2013, 7:00 AM), http://articles.washingtonpost.com/2013-07-23/politics/40862490_1_edward-snowden-nsa-programs-privacy (discussing how users were wary of information being shared in the wake of early NSA leaks by Edward Snowden).

50. *See* Rainie et al., *supra* note 1.

51. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (discussing the effects total surveillance has on society); *see also* Nicholas W. Bramble, *Safe Harbors and the National Information Infrastructure*, 64 HASTINGS L.J. 325, 337 n.42 (2013) (citing Sorrell v. IMS Health, Inc., 131 S. Ct. 2652, 2672 (2011)) ("The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure.").

significant implications for the rights to speech, association, and "intellectual privacy."[52]

Since the late 1960s, the courts have assessed the constitutionality of government searches by asking whether the defendant "exhibited an actual (subjective) expectation of privacy" at the time of the search, and whether that "expectation be one that society is prepared to recognize as 'reasonable.'"[53] Specifically, courts ask the two questions posed by Justice John Marshall Harlan in *Katz v. United States*: first, whether the defendant had a subjective expectation of privacy at the time of the search and, second, whether society generally shares that expectation.[54]

In *Katz*, the Court reviewed the constitutionality of a warrantless police wiretap of a public telephone in an enclosed glass booth.[55] The majority determined that the police violated the Fourth Amendment injunction against unreasonable searches and seizures.[56] In an opinion by Justice Potter Stewart, the Court resolved that the Fourth Amendment is addressed to "people, not places."[57] When the defendant closed the door of the booth to make his call, the Court reasoned, he had a reasonable expectation of privacy in the call.[58] This was particularly true in the context of the telephone, a communications technology that had come to occupy a "vital role" in society.[59]

Justice Harlan departed from the majority opinion to make plain that the property-based approach was inadequate to address nontrespassory government surveillance.[60] In an earlier line of cases, the Court had allowed government wiretaps of telephone conversations because the interception occurred outside of the defendant's private property.[61] The Fourth Amendment, however, was not solely addressed when addressing physical intrusions by a tangible object, Justice Harlan explained.[62] Such an approach "in

52. *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 387–389 (2008); *see also* Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 691, 693 (2013).

53. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Jones*, 132 S. Ct. at 954–55; Kyllo v. United States, 533 U.S. 27, 33 (2000).

54. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

55. *Id.* at 350 (majority opinion).

56. *Id.* at 359.

57. *Id.* at 351. In *Berger*, decided six months before *Katz*, the Court hinted that a property-based approach to privacy was insufficient when analyzing nontrespassory surveillance. *See* Berger v. New York, 388 U.S. 41, 45–49 (1967). In *Katz*, the Court overturned such an approach. *See* Katz, 389 U.S. at 359.

58. *Katz*, 389 U.S. at 351.

59. *Id.* at 352.

60. *Id.* at 360–62 (Harlan, J., concurring).

61. *Id.* at 362.

62. *Id.*

the present day," he continued, is "bad physics as well as bad law" since "reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[63]

In the end, the majority opinion and Justice Harlan's important elaboration caused "a profound shift in Fourth Amendment analysis."[64] Courts have since relied on Harlan's concurrence in particular to review a wide range of cases involving government surveillance and a wide range of technologies, including overhead flights, thermal imaging devices, drug-sniffing dogs, and GPS tracking.[65]

B. Trespass

As foundational as it is to the analysis of law enforcement surveillance techniques today, the reasonable expectation standard does not exclusively determine whether government surveillance amounts to a search under the Fourth Amendment.[66] The property-based approach has retained a place in the doctrine. Through a series of relatively recent opinions authored by Justice Antonin Scalia, the Court has relied on the explicit enumeration of tangible property in the text of the Fourth Amendment (i.e., "persons, houses, papers, and effects") to identify a property-based conception of privacy.[67]

Justice Scalia's opinion for the majority in *United States v. Jones* is the most recent articulation of this approach.[68] At issue in that case was the constitutionality of a police department's surreptitious tracking of a defendant's vehicle over the course of four weeks.[69] The Court held that attaching the GPS device and using it to track the defendant for a long period—well past the time allowed in the original warrant—constituted an unconstitutional search.[70] Writing for five members of the majority, Justice Scalia explained that the Fourth Amendment protection against searches is tied to

63. *Id.* The Fourth Amendment, Justice Harlan would elaborate four years later, required a far more searching inquiry into the relative risks of the search to citizenship in the contemporary context. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

64. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 750 (2005).

65. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414–17 (2013); Kyllo v. United States, 533 U.S. 27, 32–33 (2000); *see also* United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007).

66. United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

67. *Kyllo*, 533 U.S. at 32–33; *see also Jardines*, 133 S. Ct. at 1414; *Jones*, 132 S. Ct. at 949.

68. *Jones*,132 S. Ct. at 949.

69. *Id.* at 948.

70. *Id.* at 948–49.

common-law trespass.[71] The police officers, he concluded, intruded on the defendant's Fourth Amendment rights when they attached and used the tracking device.[72]

Justice Scalia's *Jones* opinion is not the first time he has asserted that the trespass rule is at the core of the Fourth Amendment right. *Kyllo* involved a thermal-imaging device that police used on a public street to measure heat emanating from inside a home.[73] (High temperatures suggest that the inhabitant has an indoor greenhouse or, more specifically, is growing marijuana.) Justice Scalia explained on behalf of the majority that privacy in the home was the "minimum expectation" under the Fourth Amendment.[74] The home, he continued, has long been recognized by society as "a constitutionally protected area."[75] In *Florida v. Jardines*,[76] a much more recent case involving the use of drug-sniffing dogs just outside of a home, Justice Scalia, again writing for the Court, observed that private homes are where "privacy expectations are most heightened."[77] The home, he wrote, "is first among equals" in Fourth Amendment analysis.[78]

C. Nontrespassory Surveillance

In concurring opinions, Justices Sotomayor and Alito agreed with the majority's decision in *Jones*.[79] But their opinions help clarify the scope of the current doctrine as it relates to total surveillance.

Justice Sotomayor agreed that the trespass rule represented "an irreducible constitutional minimum" of constitutional protection.[80] She, however, also would have held that an unreasonable search occurs whenever the government collects "a substantial quantum of intimate information about any person whom . . . in its unfettered discretion, [it] chooses to track."[81] The trespass rule alone, she explained, has very little applicability today, in the era of total surveillance.[82] The government's "unrestrained power to assemble

71. *Id.* at 950 (citing *Kyllo*, 533 U.S. at 34); *see also* United States v. Perea-Rey, 680 F.3d 1179, 1186 (9th Cir. 2012) ("The Supreme Court has explained that the role of reasonable expectation analysis in evaluating the constitutionality of searches of the curtilage is only in determining the scope of the curtilage, and not the propriety of the intrusion.").

72. *Jones*, 132 S. Ct. at 949.

73. *Kyllo*, 533 U.S. at 29.

74. *Id.* at 34.

75. *Id.*

76. 133 S. Ct. 1409 (2013).

77. *Id.* at 1414–15 (citing California v. Ciraolo, 476 U.S. 207 (1986)).

78. *Id.* at 1414.

79. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Alito, J., concurring); *id.* at 954 (Sotomayor, J., concurring).

80. *Id.* at 955 (Sotomayor, J., concurring).

81. *Id.* at 956.

82. *Id.* at 955.

data that reveal private aspects of identity is susceptible to abuse" and "chills associational and expressive freedoms."[83] She wrote her opinion to affirm that the *Katz* test only "augmented" Fourth Amendment doctrine and "did not displace or diminish, the common-law trespassory test," which, she argued, was sufficient to resolve the dispute before the Court.[84]

Justice Alito, in contrast, was sharply critical of the trespass rule. He too would have determined that the GPS-tracking technique at issue was unreasonable, but, unlike the majority, he would have asked whether the technique "involved a degree of intrusion that a reasonable person would not have anticipated."[85] Wherever the line between reasonable and unreasonable lies, he concluded, surveillance over the course of four weeks is undoubtedly unreasonable.[86]

What is more, Justice Alito continued, the trespass rule on which Justice Scalia relied was inadequate to assess emergent nontrespassory surveillance techniques like the continuous four-week GPS tracking at issue in the case.[87] The majority, Justice Alito continued, seemed to be drawing on a discredited pre-*Katz* line of cases in which nontrespassory surveillance of electronic communications was not considered a search under the Fourth Amendment.[88] The trespass rule, he explained, fails to address persistent unwanted nonphysical surveillance.[89] And worse, he continued, the rule would lead to incongruous results where, for example, attaching an electronic tracking device to a vehicle is forbidden while persistent nontrespassory physical surveillance of the defendant's movements on public roads is not.[90] In short, Justice Alito concluded, the trespass rule of privacy is beside the point in an era of total nontrespassory surveillance.[91]

Justice Scalia answered Justice Alito's concurrence by recognizing that trespass is not "the exclusive test" under the Fourth Amendment.[92] "Situations involving merely the

83. *Id.* at 956.
84. *Id.* at 955.
85. *Id.* at 964 (Alito, J., concurring).
86. *Id.* at 958, 964 (distinguishing *United States v. Knotts*, 460 U.S. 276 (1983), and holding that the use of surreptitiously planted beeper to monitor vehicle's movements on public roads was not a search).
87. *Id.* at 958 ("Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?" (internal citation omitted)); *cf.* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[A] man's home is, for most purposes, a place where he expects privacy.").
88. *Jones*, 132 S. Ct. at 959 (Alito, J., concurring) (discussing *Olmstead v. United States*, 277 U.S. 438 (1928) and other cases).
89. *Id.* at 962.
90. *Id.* at 961.
91. *See id.* at 959–61.
92. *Id.* at 953 (majority opinion).

transmission of electronic signals without trespass," he explained, "would *remain* subject to *Katz* analysis."[93] However, "Jones's Fourth Amendment rights," he observed, "do not rise or fall with the *Katz* formulation."[94] The Court is not required to employ the reasonable expectation test under the Fourth Amendment.[95] Nor, he explained, is the *Katz* analysis necessary to resolve the specific dispute before the Court.[96] Justice Alito's hypothetical scenario of persistent nontrespassory physical surveillance on public roads, he asserted, would have to be addressed if that case comes before the Court.[97] Rather, Justice Scalia concluded, the core traditional constitutional interest in protecting physical intrusions on tangible property is sufficient to invalidate the police's technique.[98]

Despite Justice Scalia's efforts, however, five members of the current Court now would recognize that persistent warrantless long-term surveillance like the one at issue in *Jones* is an unreasonable search within the meaning of the Fourth Amendment, irrespective of whether government officials committed a trespass.[99] Speaking for this shadow majority, Justices Sotomayor and Alito both explained that dramatic improvements in location-tracking technology have supplied law enforcement officials with the capacity to generate an astonishingly accurate profile of individuals based on the mosaic of information available.[100] This broad capacity imperils the traditional relationship between the government and its citizens and unsettles the continuing pertinence of the current doctrine.

State courts have now had some time to apply and to elaborate on the rule in *Jones* to cases involving GPS tracking.[101] In a

93. *Id.*; *see also id.* at 950–51 (discussing *Alderman v. United States*, 394 U.S. 165, 176 (1969)).

94. *Id.* at 950.

95. *Id.* at 950–51.

96. *Id.* at 954; *cf.* Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013) (explaining that a *Katz* analysis is not always necessary in these Fourth Amendment cases).

97. *Jones*, 132 S. Ct. at 953–54.

98. *Id.* at 952.

99. *See id.* at 954–55 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

100. *Id.* at 963–64 (Alito, J., concurring); *id.* at 955–56 (Sotomayor, J., concurring). This reasoning echoes the "mosaic theory" on which the D.C. Circuit below based its decision for defendants. United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010). According to the panel below, the government conducts a search within the meaning of the Fourth Amendment if the information that it aggregates over a certain period of time about an individual reveals facts that would otherwise have been private—that is, the information could not have been generated by human surveillance alone. *Id.* at 563–65.

101. *See* State v. Holden, 54 A.3d 1123, 1132–34 (Del. Super. Ct. 2010) (applying Delaware privacy provision in constitution); Commonwealth v. Connolly, 913 N.E.2d 356, 369–70 (Mass. 2009); State v. Zahn, 812 N.W.2d 490,

decision that rejected a Fourth Amendment challenge, for example, the Court of Appeals of Virginia held that law enforcement agents do not need probable cause to use a GPS-tracking device attached to the exterior of defendant's work van over a period of nearly a month.[102]

Among the courts that have suppressed such evidence, to contrast, most have relied on the "public exposure rationale" at the core of Justice Alito's concurrence—that citizens have a reasonable expectation of privacy in their prolonged travels on public roads.[103] At least a couple of these courts have relied on their own state constitutional provisions to reach that conclusion. Most notable among these is that the Supreme Judicial Court of Massachusetts held in 2009, before *Jones*, that officers engage in a seizure within the meaning of the privacy provision of the state constitution when they attach and use a GPS surveillance device to track a defendant's vehicle.[104] That court focused on the government's physical trespass of the vehicle.[105] Since *Jones*, the Massachusetts high court has stretched its seizure ruling to hold that a passenger with no property interest in the vehicle also has a privacy interest in being free from police tracking of the vehicle.[106] The court concluded that "a person may reasonably expect not to be subjected to extended GPS electronic surveillance by the government, targeted at his movements, without judicial oversight and a showing of probable cause."[107]

D. Contingency in the Doctrine

We might assume that there is a significant point of contention between the Court's approach in *Jones* and the one advocated by Justices Sotomayor and Alito. According to the latter, the reasonableness analysis under *Katz* is contingent on the relative social integration of the surveillance technique at issue at the time the controversy arises.[108] The late eighteenth century privacy-as-property framing, the concurring Justices posited, is not up to analyzing the nontrespassory government surveillance of today.[109]

Proponents of the trespass approach, on the other hand, assume that people have objective expectations of privacy in their property, and that this property-based expectation has remained constant

494–99 (S.D. 2012) (applying the reasonable expectation test under the Fourth Amendment, relying on Sotomayor's and Alito's concurrences).

102. Foltz v. Commonwealth, 698 S.E.2d 281, 291 & n.12 (Va. Ct. App. 2010) (distinguishing *Maynard*, 615 F.3d 544).

103. *Holden*, 54 A.3d at 1129.

104. *Connolly*, 913 N.E.2d at 369–70.

105. *Id.*

106. Commonwealth v. Rousseau, 990 N.E.2d 543, 553 (Mass. 2013).

107. *Id.*

108. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

109. *Id.* at 960.

since the founding period.[110] Expectations of privacy, Justice Scalia explained in *Kyllo*, do not "shrink" with every new advance in surveillance technology.[111] The Constitution bars any collection of information that is otherwise undetectable without a physical intrusion.[112] This rule keeps property as inviolable today as it was at the time of the Fourth Amendment's adoption. As self-conscious as the Justices have been about identifying themselves with either the reasonable expectation standard or the trespass rule, the distinction between the two approaches is not clear-cut. In his opinion for the Court in *Kyllo*, for example, Justice Scalia asserted that the rule about "constitutionally protected area[s]" like the home does not apply to "sense-enhancing technolog[ies]" already in "general public use."[113] In other words, surveillance technologies survive constitutional scrutiny to the extent the public has adopted them.

But, much more recently, in *Jardines*, Justice Scalia cursorily rejected the government's citation to the "general public use" qualification in *Kyllo*, explaining that it was not applicable to the facts in *Jardines*.[114] The government argued that "forensic dogs have been commonly used by police for centuries" and that their contemporary use is neither unreasonable nor unexpected.[115] Justice Scalia's reply was brisk: "[T]he antiquity of the tools that" police officers use, he argued, "is irrelevant" to the Fourth Amendment analysis whenever "the government uses a *physical intrusion* to explore details of the home."[116]

The "general public use" exception in *Kyllo*, however, does far more analytical work than Justice Scalia acknowledged in *Jardines*. In *Kyllo*, it could do nothing other than qualify the general claim that the use of "sense-enhancing technolog[ies]" to obtain information about the inside of the home without a warrant is *always* constitutionally suspect; with this language, the *Kyllo* Court recognized that the scope of the core privacy right under the Fourth Amendment narrows to the extent users have adopted the investigatory technique at issue.[117] In this way, the Fourth Amendment analysis under the trespass rule contemplates that users' expectations evolve as the public adopts the surveillance technology at issue.

Thus, even the trespass rule has substantial overlap with the *Katz* approach. The Court asserted in *Jardines*, no less, that it

110. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33–34 (2001).
111. *Id.*
112. *Id.*
113. *Id.* at 35.
114. *Jardines*, 133 S. Ct. at 1417.
115. *Id.*
116. *Id.* (emphasis added).
117. *Kyllo*, 533 U.S. at 34–35.

applies to "constitutionally protected area[s]" where expectations of privacy are "heightened."[118] The trespass rule addresses only places in which people reasonably expect to be *freest* from government surveillance.[119] Conversely, publicly exposed areas are presumably where expectations of privacy are at their lowest. In this framing, the trespass rule occupies just one aspect of the doctrine. This conclusion also aligns well with the series of cases involving police aerial surveillance of backyards.[120] In these cases, the question for the Court has generally been whether the overhead flight at issue is sufficiently regular and socially expected.[121] Some yards and fields are more protected than others, no matter the implications for private property ownership.

That the two approaches overlap, however, does not mean that they are not addressed to two discrete kinds of privacy interests. The trespass rule concerns private property. The *Katz* test, on the other hand, is addressed to intrusions of privacy more generally and is conditional by design.

As they both accommodate the shifting contingencies of public expectation and adoption, however, neither really clarifies how judges ought to treat problems associated with emergent techniques, including the current controversies associated with total government surveillance. Neither approach, to put the point differently, is particularly useful at answering whether the emergent surveillance techniques of today can ever go too far.

To provide that Fourth Amendment protections against warrantless government searches are as permissive as users expect them to be is not a standard at all. By pegging the test to expectation, the doctrine just recites a descriptive truism about adoption patterns and product lifecycles; firms design technologies in ways that are keyed to inchoate consumer expectation and consumers, in turn, adopt or reject those services depending on how relatively salient they are over time.[122] As such, both expectation and trespass approaches are far too contingent to be useful as a matter of positive law. The Fourth Amendment under this framing

118. *Jardines*, 133 S. Ct. at 1414 (citing California v. Ciraolo, 476 U.S. 207, 213 (1986)).

119. *Id.*

120. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450–52 (1989) (holding that police did not engage in a search of the defendant's greenhouse from a helicopter above because the inside of the greenhouse could be seen from above through the partially open sides and roof of the greenhouse); *Ciraolo*, 476 U.S. at 215 (holding that the police did not engage in a search of the defendant's yard from the aircraft above because "private and commercial flight in the public airways is routine").

121. *See, e.g.*, *Riley*, 488 U.S. at 454–55 (O'Connor, J., concurring).

122. *See generally* GEORGE M. BEAL & JOE M. BOHLEN, IOWA STATE UNIV. SCI. & TECH., THE DIFFUSION PROCESS (1981) (discussing how farmers accept new ideas).

is not a particularly useful protection if its scope is premised on the public's recognition that governments have the capacity to surveil their every move online.[123]

E. Expectation and the Third-Party Doctrine: The Problem of Cell Phone Location Tracking

A very recent line of cases in state and federal courts involving warrantless government surveillance of mobile phone location data illustrates the point. This form of nontrespassory government surveillance, unlike the direct law enforcement searches at issue in *Kyllo*, *Jones*, and *Jardines*, depends on the cooperation of the service providers who supply noncontent communication about their subscribers' phone usage.

The current doctrine has no clear answer for whether total surveillance violates the Fourth Amendment when third-party service providers collect and supply the information to law enforcement officials.[124] The doctrine is inconclusive if, on the one hand, users are willing to give their information to service providers for the purposes of administering the underlying service but, on the other hand, polls suggest that users are wary about the amount of transactional data they volunteer to providers and that governments have access to that data. As inconclusive as the current doctrine is, it is no surprise that courts have not been unanimous in their approach to cell phone location tracking.

1. Cell Phone Location Tracking

The growth of the market for wireless devices, gadgets, applications, and services over the past several years has been

123. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 25, *available at* http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf ("The chief difficulty with the reasonable expectation of privacy test is that it poses a question for which there is no good answer. . . . [J]ust because a person knows that law enforcement agents have the technological capability to access electronic communications, that does not mean he would be unperturbed to find out that they actually accessed his.").

124. This is far from the first essay or article to critique the doctrine. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007) (discussing an array of third-party issues, including subpoenas); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J. L. & POL'Y 211, 242–44 (2006) (critiquing how courts apply an "assumption of the risk" concept to the reasonable expectation of privacy framework); Freiwald, *supra* note 123, ¶¶ 8–9 (arguing that courts should move away from considering whether users actually know their communications are vulnerable and focus on the electronic surveillance method itself); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113–14 (2008) (contending that the "Stranger Principle" of collecting information from third parties threatens to completely undermine Fourth Amendment protections).

remarkable.[125] And it does not appear to be slowing down.[126] The vast majority of adults in the United States own a cell phone, and more than half own a smartphone.[127] According to one report, mobile data traffic will increase anywhere from ten to twenty-five fold in the next five years.[128] The growth rate of mobile Internet subscriptions is higher than that for wired subscriptions.[129] It was estimated that by the end of 2013, mobile device connections on our planet would outnumber people.[130]

All of these new connections will only increase the amount of data coursing through the networked information economy. Accordingly, service providers, device manufacturers, and application developers have designed smartphones and software that collect an array of transactional noncontent user data of which user location data are among the most notable.

Service providers generally collect and analyze cell phone location data to ensure, among other things, that subscribers maintain network connection.[131] But, as with the data that

125. INT'L TELECOMM. UNION, MEASURING THE INFORMATION SOCIETY 156 (2013), *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf; Claire Cain Miller, *Mobile Apps Drive Rapid Change in Searches*, N.Y. TIMES, Jan. 8, 2013, at B1; *Trend Data (Adults)*, PEW RES. INTERNET PROJECT, http://fe01.pewinternet.org/Static-Pages/Trend-Data-(Adults)/Device-Ownership.aspx (last visited Mar. 25, 2014).

126. *See, e.g.*, Ryan Knutson & Ben Fox Rubin, *Verizon Reports Slowdown in Growth*, WALL ST. J., Oct. 18, 2013, at B4 ("Verizon Wireless added 927,000 subscribers with contracts in the quarter."); Esme Vos, *Smart Meter Deployments to Double Market Revenue of Wireless Modules*, MUNIWIRELESS (Oct. 16, 2013), http://www.muniwireless.com/2013/10/16/smart-meter-deployments-double-market-revenue/ ("An increase in smart meter deployments will see the global market for wireless communication modules approximately double in value over the coming years.").

127. *Trend Data (Adults)*, *supra* note 125.

128. OECD, MACHINE-TO-MACHINE COMMUNICATIONS: CONNECTING BILLIONS OF DEVICES 5 (2012), *available at* dx.doi.org/10.1787/5k9gsh2gp043-en; *see also* David Talbot, *The Spectrum Crunch that Wasn't*, MIT TECH. REV. (Nov. 26, 2012), http://www.technologyreview.com/news/507486/the-spectrum-crunch-that-never-really-was/.

129. FED. COMMC'NS COMM'N, INTERNET ACCESS SERVICES: STATUS AS OF JUNE 30, 2012, at 1 (2013), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0520/DOC-321076A1.pdf.

130. Craig Timberg, *Mobile Device Connections Growing Quickly*, WASH. POST (Feb. 25, 2013), http://www.washingtonpost.com/business/technology/mobile-device-connections-growing-quickly/2013/02/25/ca98ea98-7f51-11e2-a350-49866afab584_story.html?wprss=rss_technology.

131. Indeed, all cellular phones are in constant contact with service-provider cell towers by design. "Cell phones use radio waves to communicate between a user's handset and a telephone network. To connect with the local telephone network, the Internet, or other wireless networks, cell-phone providers maintain an extensive network of cell sites, or radio base stations, in the geographic areas they serve." State v. Earls, 70 A.3d 630, 637 (N.J. 2013)

smartphone applications collect about users, subscriber location data have value over and above their role in keeping subscribers connected. Location information can support an array of geographically-contingent consumer applications and services. Any entity in possession of location data about users' phones has that much more information that it can use to develop accurate user profiles.

2. Third-Party Doctrine and Mobile Phone Tracking

Law enforcement and national security officials in particular have a keen interest in the location of criminal suspects and their affiliates.[132] Relatively recent reports indicate that police departments across the country have dramatically increased their requests to service providers to supply user location information.[133] Most law enforcement officials have made such requests without even bothering to obtain a warrant,[134] and service providers have generally complied.[135]

Subscribers, however, generally do not buy or use a phone service in order to be tracked by the government. Most users in the United States apparently believe that information about their

(citing *In re* U.S. Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010)) (internal citations omitted).

> Whenever a cell phone is turned on, it searches for a signal and automatically registers or identifies itself with the nearest cell site—the one with the strongest signal. The process is automatic. Cell phones re-scan every seven seconds, or whenever the signal strength weakens, even when no calls are made.

Id. (citing *In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005)) (internal citations omitted). Most manufactures also make and sell smartphones with GPS tracking technologies. Jagdish Rebello, *Four out of Five Cell Phones to Integrate GPS by End of 2011*, IHS TECH. (July 16, 2010), https://technology.ihs.com/388892/four-out-of-five-cell-phones-to-integrate-gps-by-end-of-2011.

132. *See* James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES, Sept. 29, 2013, at 1; Savage, *supra* note 5.

133. *See* Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1.

134. *See id.*

135. No service provider has ever objected to complying with court orders for foreign communications, for example. *See In re* Application of the F.B.I. for an Order Requiring the Production of Tangible Things from [redacted], NO. BR 13-109, at 15–16 (FISA Ct. 2013), *available at* http://s3.documentcloud.org/documents/791759/br13-09-primary-order.pdf. By its own account, the FISA Court has granted over 99% of NSA applications (some after court-ordered modification) for user data. Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Charles E. Grassley, Ranking Member, Senate Comm. on the Judiciary (Oct. 11, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/ranking-member-grassley-letter-131011.pdf.

mobile phone usage ought to be private.[136] Yet, service providers and governments have forged a public-private collaboration through which law enforcement officials obtain location information about user accounts.

That this surveillance occurs in furtherance of law enforcement investigations removes it from the business purpose for user location tracking and into the higher stakes zone of state action that is subject to constitutional scrutiny.[137] The courts have applied the third-party doctrine to analyze the constitutionality of public-private collaborations like these. Under the doctrine, governments may rely on information that defendants knowingly volunteer to third-party witnesses to a communication.[138] The courts have applied this general rule to cases in which law enforcement officials monitor the information that, for example, banks and telecommunications service providers obtain from customers in the ordinary course of business.[139]

Smith v. Maryland, a case from 1979 involving telephone landlines, remains the defining statement by the Court on the third-party doctrine as applied to telecommunications service providers.[140] There, defendant Smith had made harassing phone calls to a victim.[141] Law enforcement officials confirmed that Smith was responsible for these calls after attaching a pen register to his home phone line.[142] Smith sought to suppress the use of the phone record at trial.[143] The Court rejected the motion, explaining that Smith did not have a reasonable expectation of privacy in the phone company's record of the call since he knowingly gave that information to the company when he dialed the phone numbers.[144] Tracking devices, the Court explained, are routinely used by service providers in order to check billing, detect fraud, block harassing calls, and prevent violations of law generally.[145]

a. Real-Time Location Data

Courts have relied on this doctrine to determine whether law enforcement surveillance of real-time (or prospective) and historical

136. *See* JENNIFER M. URBAN ET AL., MOBILE PHONES AND PRIVACY 2 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

137. *See* NAACP v. Alabama, 357 U.S. 449, 460–61 (1958).

138. *See* United States v. White, 401 U.S. 745, 749 (1971).

139. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741–43 (1979); United States v. Miller, 425 U.S. 435, 438–40 (1976).

140. *Smith*, 442 U.S. 735.

141. *Id.* at 737.

142. *Id.*

143. *Id.* at 737–38.

144. *Id.* at 744 (discussing *Miller*, 425 U.S. at 442–44 and holding that there is no reasonable expectation of privacy in bank records held in the ordinary course of business).

145. *Id.* at 742.

cell-site location data requires a showing of probable cause.[146] As to the former, courts have disagreed about whether governments must make a showing of probable cause before obtaining the evidence. In one line of cases, courts have cited *Jones* to distinguish between short-term and long-term tracking, which causes "foreseeable intrusion into protected areas."[147] That is, courts in this line of cases have determined that police may obtain real-time cell phone location information to the extent the police otherwise could have tracked the defendant in public places.[148] In *United States v. Skinner*, for example, the Sixth Circuit panel distinguished *Jones* by observing that the three days of tracking at issue in the case before it did not last as long and was not as comprehensive.[149] Along these lines, a district court in that jurisdiction cited *Skinner* approvingly (as it must) but found that a seven-month-long tracking of a defendant's phone presented the same "concerns regarding extreme comprehensive tracking raised in *Jones*."[150]

These courts have assumed that defendants volunteer their phone location information when they procure and use the phone.[151] Discussing *Smith*, for example, a judge in the Eastern District of New York recently explained "that the voluntary disclosure doctrine provides the most important departure point in evaluating requests for prospective data."[152] It is not a defense that defendants do not control or know about the role of the third-party service provider.[153] "[I]t is clearly within the knowledge of cell phone users," that court explained, "that their telecommunication carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time."[154] At least one other trial court in the district agrees.[155]

146. *See* United States v. Powell, 943 F. Supp. 2d 759, 773 (E.D. Mich. 2013); *In re* Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 78 n.4 (D. Mass. 2007).

147. *Powell*, 943 F. Supp. 2d at 780; *see also* United States v. Skinner, 690 F.3d 772, 777–78 (6th Cir. 2012).

148. *Skinner*, 690 F.3d at 777–78.

149. *Id.* at 779–80; *see also* United States v. Forest, 355 F.3d 942, 950–52 (6th Cir. 2004), *remanded on unrelated sentencing grounds sub. nom* Garner v. United States, 543 U.S. 1100 (2005); United States v. Navas, 640 F. Supp. 2d 256, 263–64 (S.D.N.Y. 2009), *rev'd on other grounds*, 597 F.3d 492 (2d Cir. 2010); Devega v. State, 689 S.E.2d 293, 300–01 (Ga. 2010).

150. *Powell*, 943 F. Supp. 2d at 774.

151. *See, e.g.*, *Skinner*, 690 F.3d at 777; *In re* Smartphone Geolocation Data Application, No. 13-MJ-242 GRB, 2013 WL 5583711, at *13 (E.D.N.Y. May 1, 2013).

152. *In re Smartphone Geolocation Data Application*, 2013 WL 5583711, at *13.

153. *Id.* at *14.

154. *Id.*

155. *See In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011).

Some U.S. district courts, however, have pushed back against this reasoning, finding that defendants do not relinquish privacy in the real-time location simply by procuring a mobile phone.[156] A district court in Vermont, for example, explained that defendants do not volunteer their phone location data during the ordinary course of business to third parties.[157] Nor, it elaborated, do defendants "expect their cell phones to be pinged in the ordinary course of business."[158] Accordingly, law enforcement must make a showing of probable cause before obtaining real-time or prospective cell phone location information.[159]

b. Historical Location Data

There is similar disagreement among the courts about how to treat historical cell phone location data. The Fifth Circuit recently held, for example, that the Fourth Amendment does not require law enforcement officials to obtain a warrant before requesting subscribers' historical phone location information.[160] That panel explained that callers do not have a reasonable expectation of privacy in data about when or where they talk on their mobile phones because, under the third-party doctrine, service providers have an instrumental business interest in recording subscribers' transactions.[161] Subscribers voluntarily disclose information about the call to service providers in order to make the connection.[162] According to the panel, law enforcement authorities may obtain this data from service providers without first making a showing of probable cause.[163]

But again, courts are not unanimous. District courts in New York and Texas, for example, have found that the Fourth Amendment requires the police to make a probable cause showing

156. *See, e.g.*, United States v. Caraballo, No. 5:12-cr-105, 2013 WL 4039028, at *16–18 (D. Vt. Aug. 7, 2013); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005).

157. *Caraballo*, 2013 WL 4039028, at *18.

158. *Id.*

159. *Id.*; *see also* United States v. Dooley, No. 1:11-CR-255-3-TWT, 2013 WL 2548969, at *21–22 (N.D. Ga. June 10, 2013).

160. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013); *see also* United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012).

161. *In re U.S. for Historical Cell Site Data*, 724 F.3d at 610 (citing Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978)); *see also* United States v. Miller, 425 U.S. 435, 444 (1976) (applying third-party rule to records that a bank keeps in the regular course of business); United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

162. *In re U.S. for Historical Cell Site Data*, 724 F.3d at 612.

163. *Id.* at 615.

before obtaining historical cell-site data.[164] They have explained that the collection of months of cell phone location data could help render a "sufficiently detailed and intimate" profile of a suspect's movements to trigger serious constitutional concerns.[165]

Likewise, a unanimous New Jersey Supreme Court found that warrantless collection of historical cell phone data violates the privacy provision in the state constitution. "[I]ndividuals," the court explained, "do not lose their right to privacy [under the state constitution] simply because they have to give information to a third-party provider, like a phone company or bank, to get service."[166] Subscribers have a reasonable expectation of privacy in records that service providers collect to make the connection.[167] Mobile phone location data, the court explained, can be "far more revealing" than telephone records, bank records, or Internet subscriber information because they disclose "personal affairs, opinions, habits and associations."[168] This information provides new insight into where subscribers go, "the people and groups they choose to affiliate with and when they actually do so."[169] Wireless devices, as such, are little more than "24/7 surveillance" devices.[170] People do not reasonably anticipate that as much when they buy a cell phone.[171] "Although individuals may be generally aware that their phones can be tracked," the court explained, "most people do not realize the extent of modern tracking capabilities and

164. *See, e.g.*, *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20, 127 (E.D.N.Y. 2011) (seeking long-term, historical information); *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 837–40 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013); *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 579 (E.D.N.Y. 2010); *In re* Application of the U.S. for & Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location–Based Servs., 727 F. Supp. 2d 571, 583–84 (W.D. Tex. 2010); *but see* United States v. Pascual, 502 Fed. App'x 75, 80 & n.6 (2d Cir. 2012), *cert. denied*, 134 S. Ct. 231 (2013) (suggesting that, in spite of district court decisions in the Second Circuit, defendant's motion to suppress cell phone location data obtained without a showing of probable cause was probably consistent with *Smith v. Maryland*, 442 U.S. 735 (1979) and *Miller*, 425 U.S. 435).

165. *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 119.

166. State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (citing State v. Reid, 945 A.2d 26 (N.J. 2008)). *See generally* N.J. CONST. art. 1, § 7, *available at* http://www.njleg.state.nj.us/lawsconstitution/constitution.asp.

167. *Earls*, 70 A.3d at 643; *see also Reid*, 945 A.2d at 34–35 (discussing Internet service subscriber information); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) (discussing bank records).

168. *Earls*, 70 A.3d at 642 (citing *McAllister*, 875 A.2d at 866).

169. *Id.*

170. *Id.*

171. *Id.* (citing United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring)).

reasonably do not expect law enforcement to convert their phones into precise, possibly continuous tracking tools."[172]

3. Technological Design

We would do well by revisiting the particulars of the *Smith* opinion to gain insight on its applicability to contemporary mobile phone location tracking. An important but arguably underappreciated feature of the opinion is the Court's assumption about the way in which telephony works. According to the Court, subscribers had long understood that phone carriers receive and transmit calls through service providers' switching equipment.[173] It was of no consequence as a constitutional matter, the Court explained, that service providers had automated this process; all parties to the call could reasonably expect that the phone company would be privy to the communication.[174] Defendant Smith, the Court concluded, should have reasonably expected that he needed the phone company to complete the call.[175] In this way, the Court's holding reaffirmed the longstanding exception under the Fourth Amendment for third-party witnesses to a communication.[176]

Many courts have nevertheless taken the analysis in *Smith* to stand for the broad principle that there is something about noncontent information *per se* that is entitled to less protection under the Fourth Amendment than the content of communications.[177] To be sure, the *Smith* court recognized that the pen register collected noncontent information as opposed to communications content.[178] But the mere fact that the data at issue were not the contents of the communication (i.e., the harassment) was not analytically significant; as shown above, the Court viewed

172. *Id.* at 643.

173. Smith v. Maryland, 442 U.S. 735, 744 (1979).

174. *Id.* at 744–45; *see also* United States v. Knotts, 460 U.S. 276, 283–84 (1983) (automating the process of connecting a beeper service subscriber's communication is not significant for the purposes of Fourth Amendment analysis); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 600 (2011) (discussing the rationale the Court used in *Smith*, 442 U.S. 735).

175. *Smith*, 442 U.S. at 742.

176. *See* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.3(c) (5th ed. 2009).

177. *See id.* (discussing competing interpretations of *Smith*, 442 U.S. 735). The Ninth Circuit elaborated on this point in a case involving text messages, holding that users of text messaging services have a reasonable expectation of privacy in the content of their texts but not the numbers to which they are sending those texts. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008), *overruled on other grounds sub nom.* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

178. *Smith*, 442 U.S. at 741.

the sharing of noncontent data as an expected incident of how the phone company would complete his call.[179]

Courts nevertheless rely on the broader reading of *Smith*—that probable cause showings are not required to track noncontent data as a matter of course—when they review government requests to obtain noncontent electronic communication data about subscribers from service providers.[180] Federal courts have relied on this logic in order to grant such orders for less than probable cause in cases involving mobile phone records, as well as email addresses, the amount of data transmitted, IP addresses of websites visited, and other information about online user accounts.[181] The assumption, attributed to *Smith*, is that such government requests are valid even without a warrant *because* the service provider is trading noncontent data.

But there is no support for this broader reading of *Smith*.[182] The Court never asserted that the content-noncontent distinction was dispositive. At a minimum, the opinion is far more complicated than the advocates of the distinction purport. The decisive factor instead was how, according to the Court, subscribers expect the telephone technology to work.[183] The service provider makes the connection possible, the Court noted, by receiving the call from the subscriber and in turn relaying it to the addressee.[184] Subscribers accordingly do not have any expectations of privacy in the

179. *Id.* at 743 ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey [his phone] number to the telephone company in precisely the same way if he wished to complete his call.").

180. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 740–42 (2011).

181. United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008) (holding that computer surveillance techniques, which reveal email address, IP addresses, and other noncontent data, do not violate the 4th Amendament); *In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register & Trap On [xxx]Internet Serv. Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 49–50 (D. Mass. 2005); *see also* 18 U.S.C. § 3127(3) (2012) (defining "pen register"); *id.* § 3127(4) (defining "trap and trace device").

182. *Cf.* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, U. CHI. LEGAL F. 2008, at 121, 158–69; Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1402–03 (2004); Freiwald, *supra* note 180; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1578 (2004).

183. *Cf. Smith*, 442 U.S. at 442–43 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.").

184. *Id.* at 743–44.

transactional information about the communication because they volunteer that information to service providers. Users demonstrably assume that the service provider is an inevitable and necessary participant in the communication when they consent to sharing their personal information over the telephone.[185]

In any event, the broader reading of *Smith* is not useful in the era of total surveillance.[186] To be sure, the distinction between content and noncontent is coherent; the former is likelier to disclose specific details about motivations and associations that could not necessarily be gleaned from the latter. But, today, *aggregated* noncontent information about a user's mobile phone account reveals information about actual habits and associations in ways that the content of any specific individual communication cannot.[187] This deeply personal information is unrelated to the business purpose of providing the underlying telecommunications service.[188] Under the broad reading of *Smith*, however, it could be traded, no matter how orthogonal the subsequent purpose is to telecommunications service.

This is to say nothing, moreover, of the contemporary political economy of the infrastructure through which these communications pass.[189] The local phone company is no longer the "vital" gate-keeping communications monopoly it once was.[190] Any node in the vast and complex telecommunications network is a potential link in the communication and, arguably, a site where noncontent data

185. At least one writer has noted that the decisive feature of the third-party doctrine as stated in *Miller* is the "automation rationale" on which the Court relied. *See* Tokson, *supra* note 174, at 599–600. The Court assumed that the transition from human observation to automation of the telephone switch was not constitutionally significant. *Smith*, 442 U.S. at 744 ("This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."). But now that humans do not play any real part in observing or relaying the communication to addressees, users understandably do not have an expectation that they have waived their right to privacy in the call. Tokson, *supra* note 174, at 611–12.

186. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 31–32 (D.D.C. 2013).

187. *Cf.* People v. Weaver, 909 N.E.2d 1195, 1199–200 (N.Y. 2009) (discussing the data one could obtain through a GPS device).

188. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

189. *Cf.* Solove, *supra* note 64, at 753.

190. *Cf.* Katz v. United States, 389 U.S. 347, 352 (1967).

about the connection may be collected.[191] But such reasoning simply does not make any sense if privacy is to have any constitutional or positive legal meaning. Under the broad reading of *Smith*, individual users' mobile devices could always be under government surveillance from any point in the network because that is how the technology works.[192]

III. TOWARDS A NEW FOURTH AMENDMENT PRIVACY STANDARD

A. Judicial Discovery of Expectation

It is axiomatic in the United States that courts have an affirmative duty "to say what the law is."[193] The Framers crafted the Bill of Rights generally and the Fourth Amendment in particular to be an antimajoritarian check against overly intrusive state action.[194] They ostensibly did not trust law enforcement officials or elected representatives to regulate themselves.[195] Courts were to be the ultimate arbiters of whether legislative or executive action pass constitutional muster.

Accordingly, federal courts have no choice but to be fully engaged in assessing the legality of the newest technologies and engage in a normative inquiry about whether surveillance has gone too far.[196] And, indeed, from time to time, they have, designing and recalibrating federal law to accommodate emergent Internet-based technologies. We see this commonly in the substantive areas of intellectual property and telecommunications.[197] To be sure, in

191. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 813–14 (2003).

192. *See, e.g.*, Spencer Ackerman, *Fisa Court Order that Allowed NSA Surveillance Is Revealed for First Time*, THEGUARDIAN (Nov. 19, 2013), http://www.theguardian.com/world/2013/nov/19/court-order-that-allowed-nsa-surveillance-is-revealed-for-first-time.

193. Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177–78 (1803).

194. *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948).

195. *Cf.* Julie E. Cohen, *What Privacy Is for?*, 126 HARV. L. REV. 1904, 1904–05 (2013) (arguing that when legislatures balance privacy "against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser"); *see also* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 13–18 (2003); *see generally* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995) (discussing the public perception of privacy in American society).

196. *See generally* Freiwald, *supra* note 123, ¶ 9 (discussing courts' positive duty to engage in a "normative inquiry" into the scope of privacy protection).

197. *See, e.g.*, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 965 (2005) (Breyer, J., concurring) (citing Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984)); Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 1000–02 (2005) (granting *Chevron, U.S.A., Inc. v. Nat'l Res. Def. Council, Inc.*, 467 U.S. 837 (1984), deference to agency decision that broadband service is not "telecommunications service"

those areas, courts defer as matter of administrative law doctrine to the agencies to which Congress has delegated authority to interpret and implement the pertinent federal statutes (e.g., the Communications Act and the Copyright Act).[198] But courts also take seriously their responsibility to interpret or reject statutes and agency actions when they run afoul of either constitutional principles or basic requirements under the Administrative Procedure Act.[199]

There is no reason to believe that the newest surveillance technologies should be treated any differently.[200] The *Katz* and *Smith* opinions themselves are vivid illustrations of this, as unwieldy as the standards they propounded have become over time. In both, the Court provided—at the time of their respective announcements—useful blueprints for federal law on nontrespassory government surveillance for three to four decades.[201]

The *Jones* majority, however, was not so taken by its duty to say what privacy law is in the era of total surveillance. It was reluctant to revise the current doctrine based on the limited facts before it. Justice Scalia's opinion relied instead on a far more limited eighteenth century property-based aspect of Fourth Amendment doctrine that he, above anyone else, has been elaborating on his opinions for the past thirteen or so years.[202] Even in his concurrence, Justice Alito, too, threw his hands up, explaining that legislatures are far better at discerning expectations in the context of new technologies than courts are.[203]

Reticence is sometimes prudent. Article III courts generally lack the institutional capacity to resolve the polycentric scope of problems posed by new technologies.[204] They do not routinely

under the amended Communications Act); Reno v. Am. Civil Liberties Union, 521 U.S. 844, 874 (1997) (striking down on First Amendment grounds the obscenity provisions in the Communications Decency Act that extant technologies provide "less restrictive alternatives"); WNET v. Aereo, Inc., 712 F.3d 676 (2d Cir. 2013) (holding that the "transmit clause" of the Copyright Act does not forbid subscribers from watching or recording retransmitted video streams of broadcast programming on a website without the broadcasters' permission).

198. *See, e.g.*, WPIX, Inc. v. IVI, Inc., 691 F.3d 275, 277 (2d Cir. 2012) (affirming the Copyright Office's decision pursuant to *Skidmore v. Swift & Co.*, 323 U.S. 134 (1944)) deference); *see also Nat'l Cable & Telecomms. Ass'n*, 545 U.S. at 1001–02.

199. FCC v. Fox Television Stations, Inc., 556 U.S. 502, 514–15 (2009) (holding that there is no basis in the APA to subject changes in agency policy to more searching review); Verizon v. FCC, 740 F.3d 623, 635–36 (D.C. Cir. 2014).

200. *Cf.* Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404–05 (2013).

201. *See e.g.*, Freiwald, *supra* note 180, at 732–33.

202. United States v. Jones, 132 U.S. 945, 949 (2012).

203. *Id.* at 964 (Alito, J., concurring).

204. *See* Kerr, *supra* note 17, at 805–06; *see also* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards*

receive all of the evidence regarding public opinion or public adoption of contemporary surveillance techniques. Courts may receive extralegal empirical evidence from interested parties about how the public perceives emergent surveillance techniques. They may also request sua sponte that information in briefing by the parties. They may even take judicial notice of it, without much if any elaboration.[205]

But, again, there is no articulated process or positive requirement in the Fourth Amendment to discover public expectation as a matter of course. This is quite unlike other constitutional areas for which the Court has developed measures to gauge public opinion. Consider the Court's standard under the Eighth Amendment for reviewing the constitutionality of the death penalty.[206] There, it has employed an "evolving standards of decency" test that relies on, among other things, trends in state legislatures across the country.[207]

The public expectation standard under the Fourth Amendment has no such hook. It is a relatively indeterminate concept that turns on the reviewing judges' intuitions about what is or is not a reasonable public expectation. As such, it looks much more like a wide-ranging, fact-finding expedition far better suited to legislative discovery and deliberation.[208]

B. Discovering Expectation Through Public Lawmaking

The legislative process in the United States is designed to discover and articulate public priorities.[209] Legislatures and agencies generally promulgate and elaborate area-specific privacy

for Law Enforcement Access to Location Data that Congress Could Enact, 27 BERKELEY TECH. L.J. 117, 150 (2012); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. (forthcoming spring 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2384174 (discussing the need for Big Data Ethics in today's digital society). *But see* Solove, *supra* note 64.

205. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 454–55 (1989) (O'Connor, J., concurring) ("Because there is reason to believe that there is considerable public use of airspace at altitudes of 400 feet and above, and because Riley introduced no evidence to the contrary before the Florida courts, I conclude that Riley's expectation that his curtilage was protected from naked-eye aerial observation from that altitude was not a reasonable one."); United States v. Perea-Rey, 680 F.3d 1179, 1182 n.1 (9th Cir. 2012) (taking judicial notice of geography through Google Maps).

206. *Cf.* Roper v. Simmons, 543 U.S. 551, 560–63 (2005) (noting that, since the "cruel and unusual punishment" standard under the Eighth Amendment depends on "evolving standards of decency," the Court refers to the consensus among state legislatures and global national trends); Atkins v. Virginia, 536 U.S. 304, 311–12 (2002).

207. *Roper*, 543 U.S. at 560–61.

208. *Cf. Riley*, 488 U.S. at 462–65 (1989) (Brennan, J., dissenting).

209. *See* U.S. CONST. art. I, § 7, cl. 2; U.S. CONST. art. I, § 5, cl. 2.

laws by generally attending to a wider range of economic, social, and political factors than the other branches can.[210]

This is true in the context of privacy law in particular, where legislatures work "to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[211] Consider, again, that the *Jones* majority and concurring Justices invited Congress to define privacy in the context of GPS tracking, even as they wrestled with the constitutionality of the police's warrantless use of that technique.[212]

This is an especially important point as it relates to the reasonable expectation standard today. Since 1968, federal statutes have directed courts' analysis of electronic surveillance by law enforcement.[213] Indeed, Congress and federal agencies articulate privacy expectations through statutes and regulations that are addressed to specific governmental purposes. In regard to law enforcement surveillance, for example, Congress has amended or clarified the scope of privacy protections as new technologies and techniques have emerged. Consider the Wiretap Act and the Electronic Communications Protection Act ("ECPA").[214] Congress passed the first in 1968, just a year after the Court announced its decision in *United States v. Berger* and *Katz*.[215] The new law incorporated the Court's approach to nontrespassory government searches of telephone calls, imposing judicial review at all stages of a targeted police investigation.[216] It required, for example, prosecutors to identify with particularity the sought-after evidence, alleged offenses, duration of the surveillance, and applicable laws in order to obtain a court order to intercept or obtain the contents of a

210. *Cf.* Bi-Metallic Inv. Co. v. State Bd. of Equalization, 239 U.S. 441 (1915).

211. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

212. *See, e.g.*, *id.* at 962 ("[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions."); *id.* at 964 ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."). There are some similarities between Alito's statement here and Justice Scalia's notable concurring opinion in a patent case decided during the same term, in which he disavowed any portion of the Court's opinion that recited the "fine details of molecular biology" because he could not "affirm those details on [his] own knowledge or even [his] own belief." *See* Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107, 2120 (2013) (Scalia, J., concurring).

213. Before the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) tit. III, 18 U.S.C. §§2510–2522 (2012), section 605 of the Communications Act, 47 U.S.C. § 605 (2012) was the chief protection against the interception and sharing of content and noncontent information about users' communications. *Id.* That provision, however, was rarely enforced as a matter of federal law enforcement policy. *See* Freiwald, *supra* note 3, at 28–29.

214. *See* Freiwald, *supra* note 3, at 24–32 (discussing the provenance and congressional enactment of the Wiretap Act).

215. *Id.*

216. *Id.* at 15–17, 24–32.

suspect's electronic communications.[217] Prosecutors were also to demonstrate to the reviewing judge that "there is probable cause" to believe that the interception will uncover communications about the alleged offense.[218]

The Wiretap Act, however, did not anticipate the problems unique to computing, data storage, and electronic communications that would arise in the following decade.[219] Congress accordingly amended the Wiretap Act to address user privacy protections in 1986 through Title II of the ECPA, the Stored Communications Act ("SCA").[220] The strongest protections in the new law were reserved for the content of electronic communications, including e-mails.[221] The statute imposed the same procedural hurdles for the content of email that existed for telephony, with the exception of the suppression remedy.[222]

In the SCA, Congress also made it easier for the government to obtain noncontent subscriber data.[223] The statute established, for example, a mechanism through which parties, including the government, could obtain noncontent data held by service providers about a subscriber's electronic communications.[224] Law enforcement officials may obtain a court order directed at service providers for information about subscribers as long as they can identify "specific and articulable facts showing that there are reasonable grounds to believe that the contents" or records of an electronic communication

217. *See* 18 U.S.C. § 2518(1) (2012).

218. *Id.* § 2518(3)(b).

219. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONG., FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 3 (1985), *available at* http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/fgit-1985.pdf. *See generally* LAFAVE ET AL., *supra* note 176, § 4.3(b).

220. Electronic Communications Privacy Act, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (codified at 18 U.S.C. §§ 2701–2712). *See generally* Freiwald, *supra* note 3, at 47–50 (discussing the provenance and congressional enactment of the ECPA).

221. *See* 18 U.S.C. §§ 2702–2703. The statute elaborated on the distinction between the surveillance of content and noncontent data, but, rather than refer to "content" and "noncontent data," the ECPA speaks of "stored wire and electronic communications and transactional records." Electronic Communications Privacy Act, ch. 121 (title).

222. *See* United States v. Forest, 355 F.3d 942, 949–50 (6th Cir. 2004), *cert. granted, vacated sub nom.* Garner v. United States, 543 U.S. 1100 (2005). Notably, these protections do not apply to "stored" emails—that is, emails that have been opened and are no longer in transit. 18 U.S.C. §§ 2703(a), (b)(1)(B)(i); *see also* United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, vacated in part*, 352 F.3d 107 (3d Cir. 2004). *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003).

223. *See generally* 18 U.S.C. § 2703.

224. *Id.* §§ 2701, 2702(c).

"are relevant and material to an ongoing criminal investigation."[225] This is a lower standard than the probable cause required for a search warrant under the Fourth Amendment.[226]

In 1994, Congress expanded privacy protections for some forms of noncontent electronic data.[227] But, in 2001, within months of the terrorist attacks on the World Trade Center and the Pentagon, Congress passed the Patriot Act to broaden the range of noncontent data to which the "pen register" provisions in the SCA apply.[228] These provisions have been reauthorized at least three times since 2001.[229]

As complex as this scheme is, the Wiretap Act and ECPA represent just a fraction of federal statutory law on electronic surveillance of communications. Under the Foreign Intelligence Surveillance Act ("FISA") and FISA Amendments Act, for example, the National Security Agency ("NSA") reportedly monitors any suspects "reasonably believed" to be outside U.S. borders at the time.[230] Congress also has taken the lead in defining the terms of

225. *Id.* § 2703(d); *see also* United States v. Warshak, 631 F.3d 266, 291 (6th Cir. 2010).

226. *Warshak*, 631 F.3d at 291 ("Under § 2703(d), such an order shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation." (internal quotation marks omitted)).

227. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012)).

228. *See* 18 U.S.C. §§ 3123, 3127(3); *see also* 50 U.S.C. § 1861 (2012).

229. *See, e.g.*, USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended at 18 U.S.C. 1801).

230. First Amendments Act of 2008 § 702, 50 U.S.C. § 1881a(a). The agency does this by using keywords to search existing data stores of online activity. The NSA, however, has yet to publicize the names or numbers of U.S. citizens whose domestic communications have been monitored deliberately or inadvertently. The agency has acknowledged, however, that U.S. citizens' communications with foreigners are, and will continue to be, inadvertently swept into their online dragnets, particularly as the United States is the principal hub through which much of the world's Internet communications flow. *See NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (July 10, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. James Clapper, the Director of National Intelligence, has assured that the NSA employs "extensive procedures" to "minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. persons." William Saletan, *The Government's Cybersurveillance Program Targets Foreigners, Not Americans. But Can It Tell the Difference?*, SLATE (June 7, 2013), http://www.slate.com/articles/technology/technology/2013/06/prism_and_u_s_citizens_does_the_government_s_cyber_surveillance_program.html. Since widespread reporting of this practice, the Obama administration has sought to assure that the proper checks are in place to regulate unduly invasive tracking practices. The Foreign Intelligence Surveillance Court, which is responsible for oversight of NSA surveillance activity under the FISA, recently explained that it approves over 99% of applications for surveillance, a quarter of which are approved after court-ordered modification. *See* Larry

what is or is not private across legislative fields outside of electronic surveillance by law enforcement, albeit very unevenly.[231] Congress and the federal agencies responsible for implementing law have defined informed consent, opt-out, transparency, and confidentiality requirements in a wide array of legislative fields, including credit reporting,[232] health records,[233] and videotape rental information.[234]

Evidently, the public-lawmaking bodies have been attending to privacy protection for at least four decades, amending statutes along the way in order to account for emergent technologies and prevailing political preoccupations. This trend continues today. Congress, state legislatures, and federal agencies are considering a range of new privacy-related limits, for example, on online revenge posts[235] and online gun purchases,[236] as well as on trading among commercial data brokers and Internet companies of online user information.[237] Among the latter in particular are transparency

Abramson, *FISA Court: We Approve 99 Percent of Wiretap Applications*, NPR (Oct. 15, 2013, 3:57 PM), http://www.npr.org/blogs/thetwo-way/2013/10/15/234840282/fisa-court-we-approve-99-percent-of-wiretap-applications?ft=1&f=1001. Recent news reports also suggest that other national security agencies, including the Central Intelligence Agency, have paid service providers for call data. *See* Savage, *supra* note 5.

231. *See* Chris Hoofnagle, *United States of America*, *in* COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS 1 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1639161 ("A panoply of statutes now regulates specific types of government and business practices, with no broadly-applicable privacy statute governing data collection, use, or disclosure.").

232. Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2012).

233. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, § 701, 110 Stat. 1936, 1939 (1996) (codified at 29 U.S.C. § 1181).

234. 18 U.S.C. §§ 2710–2711 (2012).

235. *See, e.g.*, Erica Goode, *Once Scorned, but on Revenge Sites, Twice Hurt*, N.Y. TIMES, Sept. 24, 2013, at A11; *California Enacts, New York to Propose Criminal Laws Tackling "Revenge Porn,"* CRIM. DEF. NETWORK (Oct. 4, 2013), http://www.criminal-defense-network.com/privacy-california-enacts-new-york-propose-criminal-laws-tackling-revenge-porn/.

236. Jonathan Weisman & Jennifer Steinhauser, *Critical Week in Senate for Gun and Immigration Bills*, N.Y. TIMES (Apr. 8, 2013), http://www.nytimes.com/2013/04/09/us/politics/congress-returns-with-focus-on-guns-and-immigration-legislation.html. Of course, that policymakers are involved in defining privacy in or outside of the context of emergent technologies is not to say that they always do a good job. Public lawmaking is rife with dubious invasions of privacy on minorities.

237. *See* Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES, Oct. 31, 2013, at A3; Natasha Singer, *Citing Deep Data Collections, Senator Opens Inquiry of Information Brokers*, N.Y. TIMES, Oct. 11, 2012, at B3; Marc S. Roth & Charles Washburn, *Data Brokers Face Blurring Lines, Increased Regulatory Risks*, BLOOMBERG LAW, http://about.bloomberglaw.com/practitioner-contributions/data-brokers-face-blurring-lines/ (last visited Mar. 25, 2014); *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

rules that would require companies to make their data sharing policies public and also to provide to users all of the information that those companies hold about them.[238]

C. Towards a New Judicial Standard

Mindful of the trend towards codification, judges have eagerly invited Congress to elaborate substantive protections by statute.[239] They presume that legislatures are far better at discovering and articulating public expectations than they are.[240] To be sure, statutes also have holes that courts from time to time have filled.[241] But today, for the most part, judges and some scholars believe that legislatures are at least as good, if not better, at adapting broad privacy protections to emergent technologies.[242]

This does not mean, however, that courts do not have a central role to play in defining the scope of privacy under the Fourth Amendment.[243] To the contrary, to remove them from the governance of privacy law is to work against a foundational feature of our constitutional system. At a minimum, courts are constitutionally essential to adjudicating whether law enforcement officials in specific cases have made a sufficient probable cause showing to justify a search.[244] Courts have long weighed in on a wide range of fact-specific privacy problems associated with emergent technologies.[245]

But my argument here is not that courts should define all of privacy law. All branches have an important institutional role to play, as all of them have distinctive competencies to contribute.[246]

11–12 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

238. Singer, *supra* note 237.

239. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

240. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451–52 (1989) (concluding that because a helicopter that spotted his marijuana plant was flying at a legally permissible level, the defendant did not have a reasonable expectation of privacy).

241. Solove, *supra* note 64, at 761–65.

242. *See, e.g.*, Kerr, *supra* note 17, at 805; *see also* Richards, *supra* note 6, at 1958 (agreeing with Kerr that "federal statutory law has advantages over the Fourth Amendment in guarding against surveillance in the digital age").

243. *See* Johnson v. United States, 333 U.S. 10, 17 (1948); *see generally* Solove, *supra* note 64, at 749.

244. U.S. CONST. amend. IV.

245. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that the defendant did not have a reasonable expectation of privacy in a beeper placed in a container that was transported to the owner's cabin); United States v. Ahrndt, 475 F. App'x 656, 658 (9th Cir. 2012) (holding that the defendant had a reasonable expectation of privacy in Limewire files stored on a wireless network).

246. Kerr, *supra* note 17, at 806; Solove, *supra* note 64, at 774.

To be sure, legislatures have been working hard to define privacy rights since the late 1960s.[247] But this activity does not prove that the legislature ought to hold forth above all branches on elaborating the positive legal meaning of privacy. The relative legitimacy of any public law requires the active, coequal participation of courts as well as the Chief Executive.[248]

But this aspiration has apparently not caught on in fact. In the area of networked communications in particular, courts have expressed concerns about propounding general binding legal rules prematurely. In the area of privacy law, courts fear that they are deciding issues without the benefit of knowing whether (let alone how to determine) the public has adopted the technology at issue.[249] Even the *Jones* court was eager to receive guidance from Congress.[250] As I explain above, the majority there failed to give any real guidance on the Fourth Amendment implications of smart phone GPS tracking or cell phone location tracking.[251]

That judges today eagerly request legislative guidance on the scope of privacy protection in cases involving emergent electronic communication technologies seems to be a consequence of the way in which the Supreme Court since *Katz* has framed the governing doctrine. The reasonable expectation standard today is wholly contingent on shifting public perceptions and anxieties. As such, it is ineffective at defining clear lines for all circumstances ex ante. It is especially ineffectual today, when users are demonstrably inured to the inevitable fact that their personal data can and will be traded among commercial service providers and government agencies.[252] In

247. *See, e.g.*, Solove, *supra* note 64, at 754.

248. *See, e.g.*, Paul Horwitz, *Three Faces of Deference*, 83 NOTRE DAME L. REV. 1061, 1066 (2008); Robert A. Schapiro, *Judicial Deference and Interpretive Coordinacy in State and Federal Constitutional Law*, 85 CORNELL L. REV. 656, 664 (2000); *see also* S. 914, 2011 Leg., Reg. Sess. (Cal. 2011), *available at* http://leginfo.ca.gov/pub/11-12/bill/sen/sb_0901-0950/sb_914_bill_20110701_amended_asm_v96.pdf (proposing to amend Cal. Pen. Code 1542.5 in order to overturn *People v. Diaz*, 244 P.3d 501 (Cal. 2011), which held that search of the defendant's cell phone as an incident of his arrest does not violate Fourth Amendment)). This bill was vetoed by Governor Brown, who stated, "The courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections." Letter from Edmund G. Brown Jr., Governor of Cal., to Members of the Cal. State Senate (Oct. 9, 2011), *available at* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0901-0950/sb_914_vt_20111009.html.

249. *See, e.g.*, City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

250. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

251. *See* discussion *supra* Subpart II.E.

252. Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261, 1278 (2013) ("[L]aw enforcement

this way, the judicial quest to discover the public's expectation of privacy in any given case could prove inconclusive.

This is why the current reasonable expectation standard is not enough. This is to say that the constitutional defense should not turn alone on the extent of public adoption or use of the surveillance technique at issue. Privacy would altogether lose any positive legal meaning if judicial intuitions, polls, or adoption rates were to be its measure.[253] In this vein, courts are in urgent need of a new standard that empowers them to say what the law is in the first instance, even and especially when it might contravene adoption rates or popular expectations. To let the standard stand "as is" would effectively undercut the very idea that privacy is a domain of life that is not contingent on public opinion.

At least two reforms could cure the doctrine's current failings. The first we find in the *Jones* concurrences. There, Justices Sotomayor and Alito offered a useful elaboration of the expectations standard that would take long-term location monitoring in particular into account.[254] They would ask "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[255] In this way, the concurring Justices appear to recognize that the Fourth Amendment should not merely protect discrete instances of state overreach but also those occasions where the aggregation of isolated bits of noncontent personal information could constitute a "search" within the meaning of the Fourth Amendment.

Five members of the current Court are inclined to agree with this view.[256] So it would not be surprising if the Court adopted the view in some future case. And, assuming it does adopt this "mosaic theory," such a reform would not necessarily represent a transformative shift in the doctrine. Under the approach developed by Justices Sotomayor and Alito, public expectations would remain determinative; their view is that there is a point at which certain kinds of data aggregation or prolonged surveillance exceed expectations, and that is the point at which they would draw the line.

---

agents in the United States conduct surveillance until a statute or a court decision restricts them from doing so.").

253. In some regards, this indeterminacy is among the main concerns that animate Justice Scalia's ambition for more formal stability in Fourth Amendment doctrine.

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

255. *Id.*; *see also id.* at 962 (Alito, J., concurring).

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

But, as with the expectation standard today generally, such an approach is completely contingent and hard to predict as new technologies emerge. The scope of privacy should not be determined by contemporaneous public expectations. Such a formulation defeats the purpose of privacy itself. And as long as public expectation remains the test, courts and users will continue to let their bemusement and adoption of the newest technologies guide constitutional law. The expectation analysis allows those intermittent moments of complacence, after the technology eventually enters "general public use," to shrink privacy for future generations gradually over time to the point where it would not resemble anything we know it to be today.

An alternative approach would accordingly decouple public expectation from the privacy analysis altogether. It could assert simply that long periods of surveillance and powerful algorithms for data aggregation pose a Fourth Amendment threat to the extent the information is analyzed by law enforcement officials.[257] Under this approach, courts would attend to the way in which officials use the information, notwithstanding user expectations about officials' capacity to obtain and analyze it. In this formulation, as Justice Sotomayor explained in her concurring opinion in *Jones*, the third-party doctrine would cease "to treat secrecy as a prerequisite for privacy."[258] This reform would address head-on the fictional assumption that users have constructively consented to or assumed the risk of surveillance.[259] It is this assumption that invites the rampant trading of personal user data between service providers and governments. At the same time, this approach would allow that discrete disclosures to service providers for narrow business purposes are necessary for the delivery of new and emergent communication technologies.

Courts accordingly would bring a needed dose of reality to Fourth Amendment analysis by excising any broad assumptions about the nature of user consent in the third-party doctrine. This reform would recognize that users do not generally choose to compromise their data about their phone use (or web browsing or e-mailing) just because they disclose information for the limited purpose of obtaining telecommunications service. Participation in the networked information economy is practically a necessity today.

257. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 67 (2013).

258. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *see also* Freiwald, *supra* note 180, at 746–48; Freiwald, *supra* note 123, ¶¶ 58–75 (discussing a four factor test that would inquire into whether the surveillance was hidden, intrusive, indiscriminate, and continuous).

259. *Cf.* Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1204 (2009) (explaining that knowledge of risk does not equate to assumption of risk); Freiwald, *supra* note 123, ¶ 42.

Total surveillance seems to be a highly disproportionate toll to pay for inclusion, no matter what users' expectations are.

CONCLUSION

The reasonable expectation standard and the third-party doctrine have outlived their time and usefulness. Reform is especially urgent today, in the era of total surveillance, when data brokers and governments can aggregate and trade transactional subscriber data about electronic communications so easily. Expectations are difficult to define when everyone, it seems, shares their personal information with service providers and application developers in order to be connected.

Indeed, Fourth Amendment doctrine today has nothing to offer in the way of privacy protection when even courts are uncertain about how to define public expectation as a descriptive matter. Their doubt understandably compels them to defer to legislatures to discover what expectation ought to be as a matter of law.

As contingent as the current standard is, courts are right to defer to legislatures. But the doctrine is flawed if it has the effect of encouraging judges to seek guidance from legislatures on constitutional norms. Judicial review is the vital antimajoritarian check against excessive government intrusions on individual liberty under our constitutional scheme. Courts should therefore not pass off their duty to define privacy to the political branches. They must reform privacy law doctrine accordingly if the protection against "unreasonable searches and seizures" is to have any positive legal meaning in the era of total surveillance.