A TECHNOLOGY-CENTERED APPROACH TO QUANTITATIVE PRIVACY

David Gray[γ] & Danielle Citron[χ]

ABSTRACT

We are at the cusp of a historic shift in our conceptions of the Fourth Amendment driven by dramatic advances in technologies that continuously track and aggregate information about our daily activities. The Fourth Amendment tipping point was marked this term by United States v. Jones. *There, law enforcement officers used a GPS device attached to Jones's car to follow his movements for four weeks. Although* Jones *was resolved on narrow grounds, five justices signed concurring opinions defending a revolutionary proposition: that citizens have Fourth Amendment interests in substantial quantities of information about their public or shared activities, even if they lack a reasonable expectation of privacy in each of the constitutive particulars. This quantitative approach to the Fourth Amendment has since been the focus of considerable debate. Among the most compelling challenges are identifying its Fourth Amendment pedigree, describing a workable test for deciding how much information is enough to trigger Fourth Amendment interests, and explaining the doctrinal consequences. This Article takes up these challenges.*

Our analysis and proposal draw upon insights from information privacy law. Although information privacy law and Fourth Amendment jurisprudence share a fundamental interest in protecting privacy interests, these conversations have been treated as theoretically and practically discrete. This Article ends that isolation and the mutual exceptionalism that it implies. As information privacy scholarship suggests, technology can permit government to know us in unprecedented and totalizing ways at great cost to personal development and democratic institutions. We argue that these concerns about panoptic surveillance lie at the heart of the Fourth Amendment as well. We therefore propose a technology-centered approach to measuring and protecting Fourth Amendment interests in quantitative privacy. As opposed to proposals for case-by-case assessments of information "mosaics," which have so far dominated the debate, we argue that government access to technologies capable of facilitating broad programs of continuous and indiscriminate monitoring should be subject to the same Fourth Amendment limitations applied to physical searches.

[γ] Associate Professor, University of Maryland Francis King Carey School of Law.

[χ] Lois K. Macht Research Professor of Law, University of Maryland Francis King Carey School of Law, Affiliate Scholar, Stanford Center on Internet and Society, Affiliate Fellow, Yale Information Society Project. The authors thank everyone who generously commented on this work and particularly Richard Boldt, Susan Freiwald, Don Gifford, Mark Graber, Deborah Hellman, Renée Hutchins, Dan Markel, Neil Richards, Paul Schwartz, Christopher Slobogin, Dan Solove, Max Stearns, David Super, Peter Swire, and Peter Quint.

TABLE OF CONTENTS

INTRODUCTION

Police suspect that Stringer Bell is part of a drug conspiracy. To gather evidence connecting him to locations and events associated with that conspiracy, officers want to attach a global positioning system ("GPS") enabled tracking device to his car so they can track and record his movements.[1] They also want to deploy a bird-sized drone that would record and live-stream video of his travels by car and foot.[2] Should the officers' use of these surveillance technologies be left to their unfettered discretion? Alternatively, should they be treated as a "search," and therefore subject to Fourth Amendment regulations, perhaps including the warrant requirement? Similar questions came before the Court last term in *United States v. Jones*.[3] Although *Jones* ultimately was resolved on narrow grounds, concurring opinions indicate that at least five justices harbor broad Fourth

---

[1] *See* Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414-21 (2007) (explaining the technical function and capacity of GPS-enabled tracking technology).

[2] This hypothetical is not fanciful. Peter Finn, "Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate," WASH. POST, Jan. 23, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html. State and local police are using drones for routine law enforcement activities from catching drug dealers to finding missing persons. Posting of Jennifer Lynch to Electronic Frontier Foundation blog, Jan. 10, 2012, https://www.eff.org/deeplinks/2012/01/drones-are-watching-you. In the U.S., "50 companies, universities, and government organizations are developing and producing some 155 unmanned aircraft designs." *Id.* In 2010, expenditures on unmanned aircraft in the U.S. exceeded three billion dollars and are expected to surpass seven billion dollars over the next ten years. *Id.* By 2018, "more than 15,000 [unmanned aircraft systems] in service in the U.S., with a total of almost 30,000 [will be] deployed worldwide." *Id.*

[3] 132 S.Ct. 945 (2012).

Amendment concerns about law enforcement's growing surveillance capabilities.[4] In their view, a citizen should be able to claim Fourth Amendment privacy interests in substantial amounts of information about her public or shared activities, even if she cannot do so for any of the particulars, on the theory that "the whole of one's movements . . . reveals more–sometimes a great deal more–than does the sum of its parts."[5]

Critics and supporters agree that adopting this quantitative approach to Fourth Amendment privacy would be revolutionary. In his majority opinion in *Jones*, Justice Scalia describes some of the challenges and dangers,[6] which have been echoed in early scholarly responses.[7] Foremost, defenders of quantitative privacy must explain its doctrinal pedigree.[8] Until now, assessments of Fourth Amendment interests have been made qualitatively by referring to property rights or reasonable expectations of privacy. Defenders of quantitative privacy must chart a conceptual link to these precedents or provide compelling reasons for changing course. Defenders of quantitative privacy must also provide a workable test that law enforcement and courts can apply when deciding where to draw the Fourth Amendment line.[9] For example, the Court has held that there is no "search" if police officers use a lawfully installed tracking device to follow a suspect during the course of an afternoon.[10] By contrast, the *Jones* concurrences would hold that using a tracking device to follow a suspect for twenty-eight days constitutes a search.[11] Where along the spectrum, from an afternoon to four weeks, should we draw the boundary between conduct that is and is not a search?

This Article seeks answers to these and other questions by engaging the Information Privacy Law Project.[12] Until now, information privacy law and Fourth Amendment jurisprudence have

---

[4] *See id.* 132 S.Ct. at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

[5] United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010). *See also* Hutchins, *supra* note 1, at 450, 455-56 ("it is the quantity of information revealed by GPS-enabled tracking, not its type, [that] implicates the Constitution . . .").

[6] *Jones*, 132 S.Ct. at 953-54.

[7] *See, e.g.*, Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 110 MICH. L. REV. (forthcoming 2012) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032821).

[8] 132 S.Ct. at 954.

[9] *Id.*

[10] *See* United States v. Knotts, 460 U.S. 276 (1983).

[11] 132 S.Ct. at 964 (Alito, J., concurring).

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

largely been treated as theoretically and practically discrete fields of inquiry. Their shared interest in defining and protecting privacy warrants an end to that isolation. For nearly fifty years, scholars, activists, and policymakers have warned about the dangers of unregulated information and surveillance technologies, including their chilling effects on projects of self-development that are core to our conceptions of liberty and essential to our functioning democracy.[13] These concerns have clear Fourth Amendment salience.

As a protection afforded to "the people," the Fourth Amendment serves as a crucial constitutional bulwark against law enforcement's tendency toward a surveillance state.[14] As Justice Jackson pointed out in *United States v. Johnson*,[15] law enforcement is a competitive enterprise in which government agents will naturally seek any strategic advantage available to them.[16] Pursuit of that advantage naturally impels government agents, acting with the best of intentions, toward broader and more intrusive forms of surveillance. Our eighteenth century forebears knew well the threats posed by this natural trend.[17] Before our founding, British agents routinely abused general warrants, including writs of assistance, to subject our forefathers to the eighteenth-century equivalent of a surveillance state.[18] The Fourth Amendment responded by limiting the right of law enforcement to effect physical searches and seizures. As we argue here, granting law enforcement unfettered access to online monitoring, GPS-enabled tracking, drones, and integrated closed-circuit cameras would implicate the same Fourth Amendment interests and should therefore be subject to the same Fourth Amendment limits.

The Information Privacy Law Project also offers important practical guidance on the frontiers of quantitative privacy. Some critics of the *Jones* concurrences have argued that quantitative privacy creates insurmountable practical difficulties because it suggests a spectrum with no definite points of demarcation between conduct that is and is not a "search."[19] The target for these and

---

[13] *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

[14] Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008) (exploring the "enormous political pressure" on law enforcement to use advanced surveillance and data mining technologies).

[15] Johnson v. United States, 333 U.S. 10 (1948).

[16] *Id.* at 14.

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

[18] *See infra*, Part III.

[19] Kerr, *supra* note 7, at 25-31.

other pragmatic concerns is a case-by-case method of assessing quantitative privacy interests widely referred to as the "mosaic" approach.[20] Taking inspiration from information privacy law, we propose as an alternative a technology-based approach under which the threshold question would be whether a technology has the capacity to facilitate broad programs of indiscriminate surveillance that intrude upon reasonable expectations of quantitative privacy.[21] If it does, then its use amounts to a "search," and should be subject to the crucible of Fourth Amendment reasonableness, including the warrant requirement. As we point out, this technology-centered approach promises clear guidance for courts and law enforcement while avoiding many of the practical and doctrinal challenges that attach to the mosaic approach.

Although we elaborate and defend our technology-based approach at greater length below, it is important to be clear from the outset that nothing in these pages prohibits law enforcement from using advanced surveillance technologies to investigate and prosecute crimes. Rather, our point is that the Fourth Amendment does not grant unfettered authority for government agents to use technology capable of the sort of pervasive, indiscriminate monitoring that is characteristic of a surveillance state. Law enforcement can still use these technologies in the course of specific investigations so long as they can satisfy the demands of Fourth Amendment reasonableness that courts routinely apply to a broad range of investigative techniques, including physical searches,[22] wiretaps,[23] and use of heat detection devices.[24]

In this Article we make the case for a technology-centered approach to quantitative privacy. Part I provides a brief history of Fourth Amendment doctrine to put *Jones* and the quantitative approach to Fourth Amendment privacy in context. Part II draws from the Information Privacy Law Project to explain the threats to personality development, democratic participation, and accurate judgments posed by technologies capable of aggregating massive quantities of personal information. Part III connects this discussion to core Fourth Amendment concerns. Part IV again

---

[20] *See, e.g.*, Christopher Slobogin, *Making the Most of* Jones v. United States *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CON. L. & PUB. POL'Y __ (forthcoming 2012) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2098002); Kerr, *supra* note 7, at 1; Richard McAdams, *Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 318 (1985).

[21] In proposing a technology-based approach to quantitative privacy, we are particularly inspired by the work of Susan Freiwald. *See, e.g.*, Freiwald, *supra* note 13, at 5 (offering a technology-based approach to regulating government interference with electronic communications).

[22] Johnson v. United States, 333 U.S. 10 (1948).

[23] Katz v. United States, 389 U.S. 347 (1967).

[24] Kyllo v. United States, 533 U.S. 27 (2001).

draws on information privacy law to promote a technology-centered approach to protecting reasonable expectations of quantitative privacy. Part V responds to objections and challenges.

I. QUANTITATIVE PRIVACY IN *UNITED STATES V. JONES*

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Although not specified in the text, for at least a century after the Fourth Amendment was ratified, courts defined "search" in reference to concepts of common law trespass.[25] As a consequence, Fourth Amendment rights were linked to property rights and Fourth Amendment remedies were limited to suits in tort.[26] That began to change in the early twentieth century with a shift toward increased urbanization, transportation and communication advances, and the expansion of professionalized police forces. *Olmstead v. United States* [27]stands at the cusp.[28]

Writing for a five-justice majority in *Olmstead*, Chief Justice Taft held that intercepting telephone conversations was not a "search" under the Fourth Amendment because the technology did not require invading the home.[29] In his spirited dissent, Justice Brandeis argued that this property-based approach to the Fourth Amendment was anachronistic.[30] According to Justice Brandeis, a property-based approach left unprotected practices that, while unknown to eighteenth-century Americans, had become central to then-contemporary daily life.[31] It therefore failed to protect citizens from procedures that might not require the "force and violence" necessary to invade property, but nevertheless compromised the sanctity of citizens' thoughts, beliefs, and emotions as well as the "individual security" they invested in activities like telephone conversations.[32]

---

[25] Slobogin, *supra* note 20, at 4.

[26] Akhil Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786 (1994).

[27] 277 U.S. 438 (1928).

[28] Hutchins, *supra* note 1, at 423-24.

[29] *Olmstead*, 277 U.S. at 466.

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

[31] *Id.* at 474.

[32] *Id.* at 479 (explaining that the Framers "recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things.

Justice Brandeis's view ultimately prevailed in *Katz v. United States*.[33] There, the Court held that using a listening device to monitor telephone conversations conducted in a public phone booth constituted a Fourth Amendment "search." Over the lone objection of Justice Black, who would have stayed pat with the traditional property-based approach,[34] the Court famously held that "the Fourth Amendment protects persons, not places."[35] The Court saw the enumeration of "persons, houses, papers, and effects" as examples of circumstances in which citizens traditionally have maintained reasonable expectations of privacy rather than a comprehensive list meant to limit Fourth Amendment protection to a narrow range of physical objects and locations.[36] In the Court's view, conversations in public telephone booths deserved Fourth Amendment protection because citizens had come to expect that their telephone conversations would be just as free from government surveillance as their daily domestic routines in the home. Although phone booths are open to public view, the Court pointed out that they function as spaces of aural repose. It therefore held that citizens could expect that their communications in telephone booths would not be monitored by "uninvited ear[s]," even if they can be seen by "intruding eye[s]."[37] The alternative, declining to extend Fourth Amendment protection, would unsettle these broadly held expectations and raise the specter of a surveillance state.

After *Katz*, determining whether government conduct constitutes a Fourth Amendment "search" turns on whether the person claiming offense subjectively manifested an expectation of privacy that society is prepared to recognize as reasonable.[38] Of course, we enjoy a broader range of reasonable privacy expectations in some places than we do in others.[39] For example, we harbor broad expectations of privacy in our homes, persons, and immediate possessions.[40] By contrast, the

---

They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men.").

[33] 389 U.S. 347 (1967).

[34] *Id.* at 365 (Black, J., dissenting).

[35] *Id.* at 351.

[36] The majority opinion in *Katz* did not purport to displace the property-based approach to the Fourth Amendment, but, rather, to augment it. *See id.* at 351-59. That view recently was reiterated by the majority in *Jones*, 132 S.Ct. at 950.

[37] *Katz*, 389 U.S. at 352.

[38] *See Jones*, 132 S.Ct. at 950.

[39] *See*, Slobogin, *supra* note 20, at 5.

[40] *Kyllo*, 533 U.S. at 40.

Court has ruled that we have no reason to expect privacy in activities "knowingly exposed to the public."[41] Between these endpoints, we have "diminished" expectations of privacy in our cars[42] and businesses[43] because our activities there are often, but not always, exposed to the public and regulators. As *Katz* shows, however, the key question in Fourth Amendment cases is not where a search occurs, but whether and to what degree it invades reasonable expectations of privacy.

The Court has created two important legal doctrines in the wake of *Katz*. First, it has held that law enforcement can freely make observations from any place where they lawfully have a right to be.[44] Police officers thus may stand on the street and observe us through open windows, look down on us from public airspace,[45] and monitor our movements on public roads.[46] Second, the Court has ruled that the Fourth Amendment cannot save us from ill-placed trust in third parties.[47] Even if we avoid public exposure by only sharing our private activities with a select few, there is always a risk that those people will violate our faith in them by sharing the details with law enforcement. Applying this rule, the Court has held that the Fourth Amendment does not prohibit the government's drawing benefit from privately recorded conversations,[48] "pen registers" of telephone calls,[49] or a list of financial transactions.[50] Part of the reason the quantitative approach to privacy suggested by the *Jones* concurrences is regarded as radical is because it appears to threaten these doctrines.[51]

In *Jones*, an inter-agency group of law enforcement officers suspected that Jones was a high-level participant in a conspiracy to distribute narcotics in and around the District of Columbia.[52] Jones was frustratingly cautious, however, which prevented officers from developing enough direct

---

[41] *Katz*, 396 U.S. at 351.

[42] Wyoming v. Houghton, 526 U.S. 295, 300, 305 (1999).

[43] Berger v. New York, 388 U.S. 41, 64 (1967).

[44] Florida v. Riley, 488 U.S. 445 (1989).

[45] California v. Ciraolo, 476 U.S. 207 (1986).

[46] United States v. Knotts, 460 U.S. 276, 281-82 (1983).

[47] United States v. White, 401 U.S. 745 (1971).

[48] *Id.*

[49] Smith v. Maryland, 442 U.S. 735, 742 (1979).

[50] California Banker's Assoc. v. Shultz, 416 U.S. 21 (1974). As Part IV discusses, Congress passed legislation to protect the privacy of some of those activities because the Fourth Amendment did not.

[51] As we argue below, our technology-centered approach does not disrupt this doctrine. *See infra* Part V.C.

[52] 132 S.Ct. at 948.

evidence to justify his arrest and prosecution. Officers did, however, have enough evidence to apply for warrants allowing them to "tap" his telephone and monitor his movements with a GPS device, which they attached to his Jeep.[53] These efforts produced several incriminating statements and over 2,000 pages of tracking data showing that Jones made regular visits to stash houses and other locations tied to the broader drug conspiracy during the twenty-eight day monitoring period.[54] Unfortunately, the officers did not conform to the demands of their warrant when installing the GPS device, which left the door open for Jones to object to the introduction of this evidence at trial.[55]

The trial court denied Jones's motion to suppress on the grounds that the surveillance conducted with the GPS device did not constitute a Fourth Amendment search because it revealed nothing more than activity that Jones knowingly exposed to the public.[56] The court reasoned that because the officers were not obliged to get a warrant in the first place, they could not be held to account for violating the terms of the superfluous warrant they had.[57] The court based its ruling on *United States v. Knotts*, which held that using a beeper to track a suspect's movements along public roads was not a "search" because the technology only collected information about his public movements, which the officers could just as well have obtained by "tailing" him.[58] Although the GPS device used by the agents in *Jones* provided more precise location information than the beeper in *Knotts*, the court found that the GPS-enabled tracking raised no new Fourth Amendment issues.

Jones was convicted in part based upon the GPS data, which provided a critical link between him and the alleged drug conspiracy.[59] On appeal, the United States Court of Appeals for the District of Columbia Circuit reversed.[60] Writing for the panel, Judge Ginsburg argued that *Knotts* did not sanction the long-term, twenty-four-hour electronic monitoring to which Jones was subjected.[61] According to Judge Ginsburg, *Knotts* "held only that 'a person traveling in an automobile on public

---

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id. See also infra* Part V.C. (explaining how the technology-centered approach can distinguish *Knotts* from cases like *Jones*).

[59] 132 S.Ct. at 949.

[60] *Id.*

[61] United States v. Maynard, 615 F.3d 544, 556 (2010).

thoroughfares has no reasonable expectation of privacy in his movements from one place to another,' not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end."[62]

In Judge Ginsburg's view, there is a clear difference between short-term and long-term monitoring.[63] Although movements in public can be observed in discrete time slices by law enforcement and anyone else, "the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil."[64] That is, individuals have no reason to believe that they are under constant surveillance by any particular person or entity,[65] and therefore they have a reasonable expectation that they are free from constant government surveillance as well. Judge Ginsburg further explained that people do not invest much of themselves and their identities in any given activity, such as a trip to the store. By contrast monitoring "the whole of one's movements"[66] reveals not just more of what one does, but more of who one is by painting "an intimate picture of [one's] life."[67] There is, in short, a difference between being seen and being watched.[68] For these reasons, the circuit court vacated Jones's conviction,[69] holding that, although Jones lacked a discrete Fourth Amendment interest in most of his public movements on an individual basis, he had a "reasonable expectation of

---

[62] *Id.* at 557.

[63] *Id.*

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

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

[66] 615 F.3d at 558-59.

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

[68] We are in debt to Bill Piermattei for this pithy phrasing.

[69] According to its decretal paragraph, the court "reversed" Jones's conviction, but one assumes that the court intended to leave open the possibility of a retrial if the government chose to retry Jones without evidence obtained by the GPS-enabled monitoring. *See, e.g.*, *Maynard*, 615 F.3d at 568 ("To be sure, absent the GPS data a jury reasonably might have inferred Jones was involved in the conspiracy.").

privacy in his movements over the course of a month, and use of the GPS device defeated that reasonable expectation."[70]

The Supreme Court unanimously affirmed.[71] The majority opinion, written by Justice Scalia and joined by Chief Justice Roberts with Justices Kennedy, Thomas, and Sotomayor, held that the installation of the GPS device involved a search because it was accomplished by a trespass and therefore required a warrant.[72] Although the investigating officers had a warrant, they violated its terms, rendering the installation unreasonable.[73] The majority left for another day the question of whether the continuous monitoring also constituted a search. The concurring opinions, however, left little doubt about who will win that day when it comes.

For himself and Justices Ginsburg, Breyer, and Kagan, Justice Alito concurred in *Jones* to express his skepticism of the majority's property-based approach and his preference for a quantitative approach to evaluating Fourth Amendment privacy in the face of new surveillance technologies.[74] For Justice Alito, the driving concern raised by emerging surveillance technologies is scale. "In the pre-computer age," he points out, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[75] Continuous surveillance by traditional means was logistically difficult and prohibitively expensive. Its rarity provided citizens with good reason to expect that they would generally be free from continuous surveillance and therefore could enjoy a substantial degree of anonymity in the aggregate of their public activities.[76] Although "short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," Justice Alito asserted, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[77]

---

[70] *Id.* at 563.

[71] *Jones*, 132 S.Ct. at 954.

[72] *Id.* *See also* United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) ("when the Government *does* engage in a physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.").

[73] Judge Kavanaugh proposed trespass as a narrower ground for decision in his dissent from the Circuit Court's denial of the petition for rehearing en banc. *See* United States v. Jones, 625 F.3d 766, 769-71 (2010) (Kavanaugh, J., dissenting).

[74] *Jones*, 132 S.Ct., at 957 (Alito, J., concurring).

[75] *Id.* at 963.

[76] *Id.* at 963-64. *See also* Hutchins, *supra* note 1, at 455-56.

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

Justice Alito's alternative holding would require modifying the rule that law enforcement officers have an unfettered right to observe anything they can see from a lawful vantage point. The modification he proposed would focus instead on the quantum of information produced in a particular case.[78] As a consequence, he appears comfortable with granting unfettered discretion for law enforcement to use GPS-enabled tracking or other surveillance technology on a short-term basis because only a discrete amount of information could be gathered.[79] He would require judicial review for longer-term monitoring, however, where more information would be gathered.[80]

This case-by-case methodology for evaluating quantitative privacy interests has been described as the "mosaic" approach.[81] The critical question for this approach is whether the mosaic of personal information developed by investigators in a given case violates reasonable expectations of public anonymity held by most people. Responding to that question on the record before him, Justice Alito declined to "identify with precision the point at which the tracking of [Jones's] vehicle became a search," but thought it clear that "the line was surely crossed before the 4-week mark."[82]

Justice Sotomayor wrote a separate concurrence in *Jones* to express her support for the majority's ruling and her sympathy with Justice Alito's quantitative approach to Fourth Amendment privacy.[83] Rather than adopt his case-by-case mosaic approach, however, Justice Sotomayor seemed more interested in technology. As she explained, unlike other surveillance technologies "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[84] Because GPS technology "mak[es] available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," she worried that it is "susceptible to abuse."[85] On Justice Sotomayor's view, these features

---

[78] *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

[79] *Id.*

[80] *Id.*

[81] *See Maynard*, 556 F.3d at 562; Kerr, supra note 7, at 1. The term "mosaic" is borrowed from national security law, where the government has defended against requests made under the Freedom of Information Act on the grounds that when otherwise innocuous information is aggregated it can reveal secret methods and sources. *See generally* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

[82] *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

[83] *Id.* at 954 (Sotomayor, J., concurring).

[84] *Id.* at 955.

[85] *Id.* at 956.

make GPS technology particularly intrusive. Its use would therefore implicate the Fourth Amendment, because "[a]wareness that the Government may be watching chills associational and expressive freedoms," and "alter[s] the relationship between citizen and government in a way that is inimical to a democratic society."[86]

In addition to modifying the doctrine giving law enforcement officers an unfettered right to observe anything they can see from a lawful vantage point, Justice Sotomayor suggested in her *Jones* concurrence that a doctrine of quantitative privacy may require "reconsider[ing] the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[87] In our digital age, she observed, individuals have no choice but to reveal a large amount of information to third parties. They inevitably reveal detailed information to cell phone companies, Internet service providers, search engines, social network sites, and services like OnStar. Because these technologies inevitably involve the collection, use, and sharing of mass quantities of personal information, Justice Sotomayor suggested that the third-party doctrine raises the same surveillance concerns that inhere in direct government monitoring.[88]

We favor a technology-centered approach to quantitative privacy along the lines sketched by Justice Sotomayor. In the remainder of this Article, we argue that this approach has deep doctrinal roots in the Fourth Amendment and offers clear guidance to courts and law enforcement going forward. By contrast, the mosaic approach is conceptually and practically fraught. Throughout, our analysis takes cues from the Information Privacy Law Project. In Part II, we draw on information privacy scholarship and literature to explain the critical role of quantitative privacy in the preservation of individual autonomy and a free and democratic society. In Part III, we expose doctrinal links between these insights and the Fourth Amendment.

II. LESSONS FROM THE INFORMATION PRIVACY LAW PROJECT

Although concerns about quantities of data are fairly new in the Fourth Amendment context, they have long been the focus of the Information Privacy Law Project. In the 1960s, public and private entities began to generate computerized dossiers of people's activities that armies of investigators could never have accumulated on their own.[89] Businesses digitized employment,

---

[86] *Id.*

[87] *Id.* at 957.

[88] *Id.*

[89] ALAN F. WESTIN, PRIVACY AND FREEDOM 158-63 (1967).

customer, and medical records; government generated digital records on millions of Americans, including so-called "subversives," Social Security participants, and public benefits recipients; and direct-mail companies categorized consumers and sold their personal information widely.[90]

Widespread public anxiety soon emerged about so-called "Big Brother" computer databases. From 1965 through 1974, nearly fifty congressional hearings and reports investigated a range of data privacy issues, including the use of census records, a proposed National Data Center, access to criminal history records, employers' use of lie detector tests, and the military and law enforcement's monitoring of political dissidents.[91] State and federal executives spearheaded investigations of surveillance technologies. By the late 1960s, popular culture and public discourse was consumed with the "data-bank problem."[92]

This was not lost on the courts. In *Whalen v. Roe*,[93] a 1977 case involving New York's mandatory collection of prescription drug records, the Supreme Court suggested strongly that the Constitution contains a right to information privacy based on substantive due process.[94] Although it held that the state prescription drug database did not violate the constitutional right to information privacy because it was adequately secured, the Court recognized an individual's interest in avoiding disclosure of certain kinds of personal information.[95] Writing for the Court, Justice Stevens noted the "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[96] In a concurring opinion foreshadowing Justice Sotomayor's opinion in *Jones*, Justice Brennan warned that the "central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[97]

---

[90] NATIONAL ACADEMY OF SCIENCES, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY (1972). Columbia University Professor of Public Law Alan Westin, serving as Director of the National Academy of Science's Computer Science and Engineering Board, helped lead the study of governmental, commercial, and private organizations using computers to amass dossiers on individuals, featuring 14 case studies after visiting and interviewing 55 organizations. *Id.* at 5.

[91] REGAN, *supra* note 12, at 7 (1995); NATIONAL ACADEMY OF SCIENCES, *supra* note 90, at 4-5.

[92] REGAN, *supra* note 12, at 13; NATIONAL ACADEMY OF SCIENCES, *supra* note 90, at 4-5.

[93] 429 U.S. 589 (1977).

[94] *Id.* at 599.

[95] *Id.* at 599-600.

[96] *Id.* at 605.

[97] *Id.* at 601.

Despite these early engagements, information privacy law and theory remained relatively underdeveloped through the 1970s. In the intervening years, commentators and policymakers helped fill that void. The foil for this work was the specter of a surveillance state—fueled by advances in information technology—and its effects on those it watches. As information privacy scholars have argued, continuous surveillance alters the way that people experience public life.[98] "Dataveillance"—the systematic use of data systems to monitor individuals—can cover nearly every aspect of a person's offline and online activities.[99] As Daniel Solove observes, it can generate a comprehensive picture of our identities.[100] Technologies implicated in dataveillance, including data broker databases,[101] significantly alter the balance of power between individuals and powerful entities.[102] Individuals are mostly powerless and vulnerable to the whims of those who control their information.[103] This power imbalance shapes the social atmosphere in which people live, including the dynamics and consequences of self-exposure.[104]

---

[98] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE 141 (2012).

[99] David Lyon, *From Big Brother to the Electronic Panopticon*, in THE ELECTRONIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 57-80 (David Lyon ed. 1994). Roger Clarke offered the term "dataveillance" as a way to conceptualize new forms of surveillance facilitated by the widespread use of computer-based technology. Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. OF ACM 498 (1988). Clarke identified two forms of dataveillance: (1) personal dataveillance, which involves identifiable persons who by their actions have attracted the attention of the panoptic system, and (2) mass dataveillance, which refers to gathering of data about groups of people with the intention of finding individuals requiring attention.

[100] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 33 (2008); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 44-47 (2004).

[101] Commercial data brokers provide access to thousands of data points about millions of individuals. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 248 (2006). Companies like ChoicePoint and Acxiom maintain websites custom-tailored for law enforcement that provide access to massive digital dossiers. As an internal document from the United States Marshals Service notes, "With as little a first name or partial address, you can obtain a comprehensive personal profile in minutes" with Social Security numbers, known addresses, vehicle information, telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapon permits, liens, lawsuits, marriage licenses, and the like. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 596 (2004). Data brokers now combine that information with social media activity scrapped online, store purchases, and online surfing habits culled from online advertisers.

[102] Hoofnagle, *supra* note 101, at 596.

[103] SOLOVE, UNDERSTANDING, *supra* note 100, at 108.

[104] *Id.* at 179; Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 195 (2008). Studies have shown that people experience anxiety about being watched and misunderstood. Stuart A. Karabenick & John R. Knapp, Effects of Computer Privacy on Help-Seeking, 18 J. APPLIED SOC. PSYCH. 461 (1988).

Dataveillance can impact individuals' activities, shape their preferences, and ultimately affect self-development.[105] Even when people are not sure if they are being monitored, they may internalize the notion of being watched.[106] According to Julie Cohen, continuous monitoring (or its possibility) constrains "the acceptable spectrum of belief and behavior," which can result in a "subtle yet fundamental shift in the content of our character."[107] It nudges people towards the benign, mainstream, and institutionally accepted, threatening "not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[108] Under persistent surveillance, people curtail their movements, speech, and engagements with religious, political, and ethnic groups.[109] Those who refuse to self-censor often face significant social and even financial costs. For example, during the 1950s and 1960s,[110] civil rights, antiwar, and communist activists included on the FBI's "suspicious persons list" lost jobs, work opportunities, and licenses.[111] Labor union organizers assumed new names and Social Security numbers due to fierce hostility to union members.[112]

Today's surveillance technologies pose even greater threats to liberty than the "Big Brother databanks" of the 1960s. Information gathering is quicker, cheaper, and more comprehensive than

---

[105] See Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 416-17 (2008) (offering a powerful normative justification of information privacy for intellectual development).

[106] SOLOVE, UNDERSTANDING, *supra* note 100, at 109.

[107] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425-26 (2000).

[108] *Id.*

[109] Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143-44 (2007); Christopher Sloblogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 253-55 (2002). As Justice William O. Douglas observed, "Monitoring if prevalent, certainly kills free discourse and spontaneous utterances." United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting). This is not to suggest that the surveillance of groups is justiciable, although it may be so in circumstances where the chilling of expressive association is accompanied by objective harm, such as reputational damage. *See* Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance, and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 656-57 (2004); Laird v. Tatum, 408 U.S. 1 (1972) (refusing to find justiciable constitutional violation for army's data gathering about political group because allegations of "subjective 'chill'" based on possibility that army may "at some future date misuse the information" are "not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm").

[110] S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 679-732 (1976); *see also* Lawrence Rosenthal, *First Amendment Investigations and the Inescapable Pragmatism of the Common Law of Free Speech*, 86 IND. L. J. 1, 37 (2011) (explaining that the COINTELPRO era was not an isolated abuse and was part of a sustained effort to monitor unpopular groups).

[111] *Id.* at 40. *See* DANIEL J. SOLOVE AND PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 525 (4th ed. 2012).

[112] NATIONAL ACADEMY OF SCIENCES, *supra* note 90, at 40, 41 (noting that in 1972 the Social Security Agency ("SSA") permitted individuals to assume different identities and new Social Security numbers so that they could avoid prejudice due to their group affiliations).

ever before. Whereas information gathered by public and private entities once typically remained in information silos, it is now seamlessly shared with countless organizations via the Internet.[113] Bias against groups can be, and is, embedded in data-mining algorithms, systematizing it in ways that may be difficult to eradicate.[114]

With these concerns in mind, information privacy scholars argue that "privacy in public" is indispensible for self-development, public life, and a functioning democratic society.[115] Privacy has long been a centerpiece in democratic theory because it preserves essential space for the development of ethically grounded citizens capable of engaging in the critical functions of public citizenship.[116] By definition, democratic governments are subservient to their citizens.[117] That relationship assumes that citizens come to the democratic process with at least a provisional set of moral commitments and ethical goals that they seek to advance and defend.[118] Surveillance states are undemocratic because they reverse the hierarchy of dominance, rendering citizens subservient to the state at the foundational level of personal identity.[119]

---

[113] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1459 (2011).

[114] Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 358 (2008) (explaining that bias can be embedded in human-created profiles encoded in computer algorithms, as well as in human-compiled datasets of terrorists that predictive data-mining tools would search).

[115] Aside from the consequential effects of surveillance technologies, privacy scholars also emphasize deontolotical concerns, notably that surveillance technologies demonstrates a lack of respect its subject as an autonomous person. For example, Stanley Benn explains that being "an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes." Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in NOMOS XIII: PRIVACY 2 (J. Roland Pennock & J.W. Chapman eds. 1971). The observed person sees herself as a knowable object, with "limited possibilities rather than infinite indeterminate possibilities." *Id.* Covert surveillance is problematic because it "deliberately deceives a person about his world, thwarting, for reasons that cannot be his reasons, his attempts to make a rational choice." *Id.*

[116] *See, e.g.*, STEPHEN BREYER, ACTIVE LIBERTY 3-5, 15-20, 66-74 (2005); MICHAEL SANDEL, DEMOCRACY'S DISCONTENTS: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY 350 (1996) (discussing democratic role for privately negotiated identities); Thomas Crocker, *From Privacy to Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. REV. (2009).

[117] BREYER, *supra* note 116, at 22-23.

[118] *See* Schwartz, *supra* note 13, at 1653 ("The health of a democratic society depends both on the group-oriented process of democratic deliberation and the functioning of each person's capacity for self-governance"). This is, of course, both too simple and ignores a broad debate among democratic theorists about the genesis of human subjectivity. For present purposes, we need not take sides in any of these contests. We can, for example, accept that human subjectivity is by nature and necessity a function of community but still rely on the fact that those engagements are, on the whole, conducted in relatively private circumstances and certainly beyond the gaze of government surveillance.

[119] *United States v. White*, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting) ("[C]oncepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on."); Schwartz, *supra* note 13, at 1654-55 ("democracy requires more than group deliberation at the a town square located

States have long used surveillance to shape or retard character by limiting conduct and expression. Jeremy Bentham, whose work was well known to late eighteenth-century Americans, described the potential of surveillance to change criminals' essential character.[120] His famous panopticon was designed to exploit that potential by subjecting offenders to constant surveillance. Michel Foucault extended Bentham's insights to describe how a whole range of public institutions use surveillance to shape subjects who internalize the norms and priorities of the institution.[121] More recently, Paul Schwartz has described the dangers to democracy posed by government surveillance of online activities. He defines "a coercive influence on decision making" as conduct that "takes over, or colonizes a person's thinking processes."[122] Drawing an analogy to the "telescreen" and "Thought Police" featured in George Orwell's *1984*, Schwartz contends that, as "people on the Internet gain a sense that their every mouse click and key stroke might be observed, the necessary insulation for individual self-determination will vanish."[123]

For these reasons, information privacy scholars have long argued that people need a degree of freedom from monitoring to develop their identities.[124] Preserving privacy allows people to engage in "meaningful reflection, conversation, and debate about the grounds for embracing, escaping, and modifying particular identities."[125] It facilitates uninhibited relationships that are crucial to personality development.[126] Free from pervasive monitoring, people can "come together to exchange information, share feelings, make plans and act in concert to attain their objectives."[127] Furthermore, as Anita Allen observes, information privacy gives people the chance to make

---

either in Real Space or in cyberspace. It requires individuals with an underlying capacity to form and act on their notions of the good in deciding how to live their lives. This anti-totalitarian principle stands as a bulwark against any coercive standardization of the individual.").

120 JEREMY BENTHAM, PANOPTICON (THE INSPECTION-HOUSE) (1791).

121 *See, e.g.*, MICHEL FOUCAULT, DISCIPLINE AND PUNISH, 195-308 (1977) (1975); MICHEL FOUCAULT, MADNESS AND CIVILIZATION: A HISTORY OF INSANITY IN THE AGE OF REASON (1988) (1964).

122 Schwartz, *supra* note 13, at 1656.

123 *Id.* at 1656-57.

124 *Id.* at 1651; Jeffrey H. Reiman, *Privacy, Intimacy and Personhood*, 4 PHIL. & PUB. AFFAIRS 323 (1975).

125 Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 754-55 (1999).

126 Oscar H. Gandy, Jr. *Exploring Identity and Identification in Cyberspace*, 14 NOTRE DAME J.L. ETHICS & PUV. POL'Y 1085 (2000).

127 EDWARD J. BLOUSTEIN, INDIVIDUAL AND GROUP PRIVACY 125 (1978).

meaningful choices about activities, preferences, and relations, and to act on them without fear of embarrassment or recrimination.[128]

Courts operating in the information privacy context have echoed concerns that broad, indiscriminate, and intrusive public surveillance threatens these liberty interests. For example, in the tort context, some judges have found that being in public does not necessarily mean that individuals have no interest in being free from continuous surveillance.[129] For instance, in *Nader v. General Motors Corporation*,[130] General Motors undertook a campaign to discredit and intimidate its well-recognized critic Ralph Nader. The company placed him under extensive public surveillance and wiretapped his telephone. In 1970, the New York Court of Appeals recognized that, although observing others in public places generally does not constitute a tort, sometimes "surveillance may be so 'overzealous' as to render it actionable."[131] As the court explained, "[a] person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing."[132]

In addition to these liberty concerns, the Information Privacy Law Project has warned that broad and indiscriminate surveillance compromises democratic values.[133] For example, Paul Scwartz reminds us that self-rule requires a "group-oriented process of critical discourse" among autonomous individuals.[134] Spiros Simitis cautions that "[n]either freedom of speech nor freedom of association nor freedom of assembly can be fully exercised as long as it remains uncertain whether,

---

[128] ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 17 (2012); Gary T. Marx, *Identity and Anonymity: Some Conceptual Distinctions and Issues for Research*, in DOCUMENTING INDIVIDUAL IDENTITY 316, 318 (Jane Caplan & John Torpey, eds. 2001).

[129] *See* Sanders v. Amer. Broadcast Co., 978 P.2d 67 (Cal. 1999) (finding that television show invaded employee's privacy by secretly videotaping her workplace conversations even though other employees could hear her because employee should not reasonably expect to be secretly recorded by journalists).

[130] 25 N.Y.2d 560 (Ct. App. 1970).

[131] *Id.*

[132] *Id.*

[133] Danielle Keats Citron, *Fulfilling Government's 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822 (2010).

[134] Paul M. Schwartz, *Privacy and Participation: Personal Information and the Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560-61 (1995). Paul Schwartz has relied on the work of constitutional theorist James E. Fleming in arguing that democracy in general and constitutional law in particular must secure the preconditions for "citizens to apply their capacity for a conception of the good to deliberat[ions] about . . . how to live their own lives." Schwartz, *supra* note 13, at 1651 (discussing James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 2-3 (1995)). Fleming calls for a deliberative autonomy that is based on moral autonomy, responsibility, and independence. 48 STAN. L. REV. at 30-34.

under what circumstances, and for what purposes, personal information is collected and processed."[135] Because continuous logging of citizens' activities chills experimentation with different or premature notions of the good, it can "short-circuit individual decision-making.[136] Joel Reidenberg therefore identifies information privacy as a "societal value and a requisite element of democracy."[137] Amplifying that conclusion, Schwartz ultimately questions whether anyone will engage in political deliberation when it "leaves finely grained data trials in a fashion that is difficult to understand or anticipate"[138] To preserve democratic values, privacy advocates have therefore pressed for laws that can prevent "state or community intimidation that would destroy involvement in the democratic life of the community."[139]

To be sure, citizens under continuous surveillance do not inevitably withdraw from civic engagement. They may engage in productive resistance[140] or disregard surveillance's risks on the view that they have nothing to hide.[141] Nonetheless, the impulse to self-censor is strong when people have no idea who is watching them and how their information will be used. This is all the more true for traditionally subordinated groups in our post-9/11 age.[142] Because minorities are particularly vulnerable to governmental suspicion and profiling, they are likely to refrain from exploring non-mainstream activities in the face of continuous surveillance.[143] The burden of self-censorship occasioned by a surveillance state is therefore borne unequally. More fundamentally,

---

135 Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 735 (1987). Interest groups like the ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, the Center on Democracy & Technology, and Future of Privacy have long underscored persistent surveillance's cost to democratic expression.

136 Schwartz, *supra* note 13, at 1656.

137 Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882-83 (2003); Joel R. Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497-98 (1995).

138 *Id.* at 1651.

139 Schwartz, *supra* note 134, at 561.

140 Kevin D. Haggerty, "Tear down the walls: on demolishing the panopticon," in THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND (David Lyon, ed. 2006).

141 DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 1 (2011).

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

143 *See, e.g.,* Katharine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 760-64 (2008). *See also* FREDERICK SCHAUER, PROFILES, PROBABILITIES, AND STEREOTYPES (2003) (exploring the problematic nature of predictive models when cued by race and gender because they are overused as markers of difference in morally problematic ways).

democratic participation just should not require heroic levels of civic courage—that is too much to ask of citizens in a free and democratic society.[144]

The Information Privacy Law Project has also highlighted problems caused by incorrect or incomplete personal information in databases. In an early case confronting these issues, United States District Judge Gerhard Gesell ordered the FBI to refrain from disseminating computerized criminal records for state and local employment, license, and benefits checks because the records were often incomplete and inaccurate and hence "clearly invade[d] personal privacy."[145] The court warned of ever more inaccuracies in databases with the "development of centralized state information centers to be linked by computer to the Bureau."[146]

Subsequent years have shown that Judge Gesell's concerns were well founded. Employers have refused to interview or hire individuals based on incorrect or misleading personal information obtained through surveillance technologies.[147] Governmental data-mining systems have flagged innocent individuals as persons of interest, leading to their erroneous classifications as terrorists or security threats.[148] Falsely flagged individuals may be subject to intense scrutiny at airports, be denied the right to access airplanes, face false arrest, or lose public benefits. The potential for damage is magnified by our "information sharing environment,"[149] which facilitates the distribution of such designations with countless public and private actors, compounding the error in ways that are difficult to detect and eliminate.

Consider the distortions generated by state, local, and federal cooperatives known as "fusion centers" that gather intelligence on "all hazards, all crimes, and all threats."[150] In one case, Maryland state police exploited their access to fusion centers in order to conduct surveillance of human rights

---

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

145 United States v. Menard, 328 F. Supp. 718 (D.D.C. 1971).

146 *Id.*

147 SOLOVE, DIGITAL PERSON, *supra* note 100, at 180. Only in exceptional cases do individuals discover their digital dossiers contain erroneous information about them. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1816 n.82 (2011).

148 Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1274 (2008) (exploring inaccuracies of automated decision-making governmental systems including "No Fly," public benefits, and "dead beat" parent matching systems).

149 Federal agencies, including the Department of Homeland Security, gather information in conjunction with state and local law enforcement officials in what Congress has deemed the "information sharing environment" (ISE). The ISE is essentially a network, with hubs known as "fusion centers" whose federal and state analysts collect, analyze, and share intelligence. *See* Citron & Pasquale, *supra* note 113, at 1443.

150 *Id.*

groups, peace activists, and death penalty opponents over a nineteen-month period.[151] Fifty-three political activists eventually were classified as "terrorists," including two Catholic nuns and a Democratic candidate for local office.[152] The fusion center subsequently shared these erroneous terrorist classifications with federal drug enforcement, law enforcement databases, and the National Security Administration, all without affording the innocent targets any opportunity to know, much less correct, the record.[153]

Work done in the information privacy law context provides ample evidence that broad programs of indiscriminate surveillance threaten both fundamental liberty interests and democratic values. Despite the critical role played by privacy concepts in contemporary Fourth Amendment doctrine, however, there has been very little interdisciplinary engagement between the Information Privacy Law Project and Fourth Amendment law and scholarship. The quantitative approach to Fourth Amendment privacy proposed by the concurring opinions in *Jones* invites us to end that isolation and the mutual exceptionalism it implies. In the next Part we accept that invitation.

III. THE FOURTH AMENDMENT FOUNDATIONS OF QUANTITATIVE PRIVACY

Although privacy concerns attached to quantities of data that have been explored by the Information Privacy Law Project have not yet played a prominent role in Fourth Amendment doctrine, the foundations are there. The Fourth Amendment was conceived, and has long served, as a bulwark against law enforcement's teleological tendency toward a surveillance state. So, too, the Fourth Amendment—on its own and in a broader constitutional context—treats privacy as essential to a functioning democracy.[154]

In the years since the Fourth Amendment was ratified in 1791, courts routinely have been called upon to evaluate the potential of emerging investigative strategies and technologies to diminish privacy.[155] When unfettered access to those practices raises the specter of a surveillance state, courts have limited their use by applying the Fourth Amendment's reasonableness standards.[156] Our technology-centered approach to protecting quantitative privacy follows a predictable doctrinal

---

[151] Nick Madigan, *Spying Uncovered*, BALT. SUN, July 18, 2008, at 1A.

[152] *Id.*

[153] *Id.*

[154] Thomas M. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303 (2010).

[155] BREYER, *supra* note 116, at 67.

[156] *See, e.g.*, *Kyllo*, 533 U.S. at 40; *Katz*, 389 U.S. at 351.

path, invoking the Fourth Amendment to guard against indiscriminate intrusions that compromise individuals' "power to control what others can come to know" about them.[157]

Like many provisions in the Bill of Rights, the Fourth Amendment's prohibition on unreasonable searches and seizures and its limitations on warrants have a reactionary story.[158] The core text of the Constitution does not provide for individual rights.[159] Although this omission was criticized during the drafting process,[160] it received particular attention during ratification when state legislatures raised concerns about the tyrannical potential of a strong federal government.[161] Their fears were not abstract. Members of these legislatures and their constituents still bore the scars of constraint and disfavor at the hands of the Crown and shared a common law consciousness shadowed by the Star Chamber and the torturous abuses of the Tower and the Church.[162] It was against these archetypes of tyranny that the Bill of Rights was drafted and adopted.[163]

The Fourth Amendment drew on these historical experiences to describe limitations on "the amount of power that [our society] permits its police to use without effective control by law."[164] During the colonial period, British officials and their representatives took advantage of writs of assistance and other general warrants, which immunized them from legal liability for their invasions,[165] to search anyone they pleased, anywhere they pleased, without having to specify cause

---

[157] BREYER, *supra* note 116, at 66.

[158] *See* NELSON B. LASSON, THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 13 (1937); Thomas Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L. REV. 979, 980 (2011).

[159] *See* LASSON, *supra* note 158, at 83.

[160] *See, e.g.*, LASSON, *supra* note 158, at 84-86; GEORGE MASON, OBJECTIONS TO THE CONSTITUTION OF GOVERNMENT FORMED BY THE CONVENTION (1787) (complaining about the absence of a "Declaration of Rights" in the constitution and expressing concerns that this omission would effectively moot the declarations of rights found in the constitutions of the states).

[161] *See* LASSON, *supra* note 158, at 83, 87-97; Clancy, *supra* note 158, at 1034-36; Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 400 (1974) ("To be sure, the framers appreciated the need for a powerful central government. But they also feared what a powerful central government might bring, not only to the jeopardy of the states but to the terror of the individual.").

[162] *See Warden v. Hayden*, 387 U.S. 294, 313 (1964); *Ker v. California*, 374 U.S. 23, 61 n.15 (1963) (Brennan, J., dissenting); *Frank v. Maryland*, 359 U.S. 360, 375 (1959); LASSON, *supra* note 158, at 24-28, 32; Clancy, *supra* note 158, at 981, 1030-44.

[163] *See* LASSON, *supra* note 158, at 13-50; Clancy, *supra* note 158, at 1002-04.

[164] Amsterdam, *supra* note 161, at 377.

[165] Amar, *supra* note 26, at 767, 774; VA. DECL. OF RIGHTS, ART. X (defining "general warrants" as warrants "whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence . . .).

or reason.[166] The Fourth Amendment thus prohibited "unreasonable searches and seizures" and insisted upon warrants issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[167]

Although the negative rights afforded by the Fourth Amendment have specific historical antecedents, the text itself evinces a broader historical purpose to protect against indiscriminate and invasive governmental practices that are characteristic of a surveillance state.[168] As Anthony Amsterdam reports, early English judges saw indiscriminate searches not as offenses against individuals but against the "whole English nation."[169] The Fourth Amendment reflects this societal focus by securing to "the people" the right against unreasonable search and seizure.[170] The Court's exclusionary rule jurisprudence effects these broad protections by punishing law enforcement in individual cases in order to deter potential future violators.[171] Thus, as Renée Hutchins has pointed out, "[t]he Fourth Amendment . . . erects a wall between a free society and overzealous police action–a line of defense implemented by the framers to protect individuals from the tyranny of the police state."[172]

Bear in mind that the tyranny animating the Fourth Amendment is not necessarily the product of evil intent. Rather, tendencies toward a surveillance state are part of the telos of law

---

[166] TEDFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 24-46 (1969); LASSON, *supra* note 158, at 51-78; Crocker, *supra* note 154, at 350-53; Clancy, *supra* note 158, at 1002-04; Amsterdam, *supra* note 161, at 367, 388-89, 398. *See also* United States v. Poller, 43 F.2d 911, 914 (2d Cir. 1930) (Hand, J.) ("the real evil aimed at by the Fourth Amendment is the search itself, that invasion of a man's privacy which consists in rummaging about among his effects to secure evidence against him.")

[167] U.S. Const., Amend. IV; Clancy, *supra* note 158, at 152-53; Amsterdam, *supra* note 161, at 388-89.

[168] *See* United States v. Di Re, 332 U.S. 581, 595 (1948) ("But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of criminals from punishment."); Johnson v. United States, 333 U.S. 10, 14 (1948) ("The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance."); Amsterdam, *supra* note 161, at 366 ("the specific incidents of Anglo-American history that immediately preceded the adoption of the amendment, we shall find that the primary abuse thought to characterize the general warrants and the writs of assistance was their indiscriminate quality, the license that they gave to search Everyman without particularized cause.").

[169] Amsterdam, *supra* note 161, at 366 n.191.

[170] U.S. Const., Amend IV; Crocker, *supra* note 154, at 309-10, 360.

[171] *See* Davis v. United States, 131 S. Ct. 2419, 2426 (2011) ("The rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations."); David Gray, Meagan Cooper, & David McAloon, *The Supreme Court's Contemporary Silver Platter Doctrine,* 91 TEXAS L. REV. __ (forthcoming 2012); David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence,* 50 AM. CRIM. L. REV. __ (forthcoming 2012); Arnold Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1263-72 (1982).

[172] Hutchins, *supra* note 1, at 444.

enforcement.[173] Efforts to ensure peace and security natural impel the state toward the most expansive and efficient means of preserving peace and security.[174] In this sense, "The Bill of Rights in general and the fourth amendment in particular are profoundly anti-government documents [in that] [t]hey deny to government . . . desired means, efficient means . . . to obtain legitimate and laudable objectives."[175] But the constraint is necessary because law enforcement, *qua* law enforcement, will naturally seek every advantage they can to catch criminals without necessarily considering the broader consequences for liberty and democracy.[176]

The specters of a tyrannical surveillance state that plagued our founding-era forebears no doubt warranted constitutional attention. Imagine living in a world in which state agents could kick down doors, enter homes, and rummage through drawers at will. Law-abiding citizens might have hoped that they would be immune from such intrusions, but that would be naïve. A state interested in maintaining its own authority and ensuring maximum security is not so discriminate. It will cut a broad swath, targeting not only criminals but also troublemakers, including political activists, academics, artists, and promoters of disfavored religions.[177] As we discussed in Part II, the threat of surveillance is a powerful tool for modifying behavior as well as character.[178] Thus illuminated, the Fourth Amendment is revealed as playing a critical role in our system of constitutional protections because it prohibits the kinds of broad programs of indiscriminate search that might render docile a people defined by their spirit of liberty.[179]

---

[173] *See* Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971); *James Madison, Speech at the First Congress, First Session: Amendments to the Constitution (June 9, 1789)*, *in* 5 WRITINGS OF JAMES MADISON 374-75 (1904) (worrying that, absent specific constraint, the federal government would revert to the use of general warrants under the "necessary and proper clause").

[174] *See* Amsterdam, *supra* note 161, at 378-79.

[175] Amsterdam, *supra* note 161, at 353.

[176] *Johnson*, 333 U.S. at 14.

[177] Individuals in these categories have always been the natural targets of tyranny. The certainly were in the founding era. *See* Crocker, *supra* note 154, at 346-50. Writs of assistance in the colonies were little more than protection of petty tyrants, who sometimes used them to retaliate against outspoken citizens. *See* LASSON, *supra* note 158, at 59-60. Things haven't changed all that much since. Abusive regimes from Asia to Africa to Europe to South America have put political opponents, intellectuals, artists, and religious leaders under surveillance, or worse. The same impulses of distrust are suffused through our politics. Nixon bugged not drug lords but the headquarters of his political rivals.

[178] *See* Cohen, *supra* note 107, at 1425-26.

[179] Crocker, *supra* note 154, at 360. *See also Florida v. Riley*, 488 U.S. 445, 466-67 (1989) (Brennan, J., dissenting) ("The Fourth Amendment demands that we temper our efforts to apprehend criminals with a concern for the impact on our fundamental liberties of the methods we use. I hope it will be a matter of concern to my colleagues that the police surveillance methods they would sanction were among those described 40 years ago in George Orwell's dread vision of life in the 1980's."). *Cf.* Lawrence v. Texas, 539 U.S. 558, 562 (2003) ("Liberty protects the person from

The same fears of broad programs of indiscriminate search that drove us to adopt the Fourth Amendment in 1791 are at stake today as law enforcement seeks unfettered access to contemporary surveillance technologies.[180] The governing standard for determining whether law enforcement conduct constitutes a Fourth Amendment "search" is described by Justice Harlan in his concurring opinion in *United States v. Katz*. Under the *Katz* inquiry, the Court will recognize a subjectively manifested expectation of privacy as "reasonable" if is an expectation that is broadly shared by most citizens, realistic in light of common social practices, and threatened by unfettered governmental intrusion. Technology capable of pervasive monitoring surely implicates reasonable and generally held expectations of privacy.

From an ethnographic point of view, it is hard to contest Renée Hutchins's observation that "the citizens of this country largely expect the freedom to move about in relative anonymity without the government['s] keeping an individualized, turn-by-turn itinerary of our comings and goings."[181] Furthermore, GPS-enabled tracking, aerial drones, data mining, and other technologies capable of facilitating pervasive surveillance are so covert that citizens can reasonably maintain these expectations. Anthony Amsterdam perhaps put it best, writing that "[t]he insidious, far-reaching and indiscriminate nature of electronic surveillance–and, most important, its capacity to choke off free human discourse that is the hallmark of an open society–makes it almost, although not quite, as destructive of liberty as 'the kicked-in door.'"[182]

Although it has not squarely addressed these threats, existing Supreme Court doctrine exhibits considerable sympathy for the proposition that emerging technologies capable of amassing large quantities of data about our activities implicate Fourth Amendment bulwarks against a surveillance state.[183] For example, in *United States v. Knotts*,[184] the Court indicated that "dragnet type

---

unwarranted government intrusions into a dwelling place or other private places. . . . Liberty presumes an autonomy of the self that includes freedom of thought, belief, expression, and certain intimate conduct.").

[180] *See* Berger v. New York, 388 U.S. 41, 64 (1967) (Douglas, J., concurring) ("I also join the opinion because it condemns electronic surveillance, for its similarity to the general warrants out of which our Revolution sprang and allows a discreet surveillance only on a showing of 'probable cause.'").

[181] Hutchins, *supra* note 1, at 455. *See also Jones*, 132 S.Ct. at 955-56 (Sotomayor, J., concurring); *Id.* at 963-64 (Alito, J., concurring)

[182] Amsterdam, *supra* note 161, at 388.

[183] *See, e.g.*, United States v. United States District Court, 407 U.S. 297, 312–13 (1972) ("[A] recognition of these elementary truths does not make employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy. . . . [*Katz*] implicitly recognized that the broad and unsuspected

law enforcement practices" might threaten broadly held privacy expectations.[185] The technological capacity to effect pervasive surveillance also appeared in *United States v. Kyllo*, which addressed the use of a heat detection device to detect invisible thermal emanations from a home. Writing for the Court, Justice Scalia emphasized that the Court must not "permit police technology to erode the privacy guaranteed by the Fourth Amendment."[186] Applying *Katz*, he gave full Fourth Amendment credit to the dangers posed by "advancing technology—including imaging technology" to enable surveillance in the home that would invade broadly held expectations of privacy. Out of fear that state agents could use then-existing technologies and "more sophisticated systems that are already in use or in development"[187] to conduct broad, indiscriminate surveillance of a whole range of activities in the home, the Court held that heat monitoring technologies should be subject to Fourth Amendment review.[188]

As is clear from historical context, constitutional text, and doctrine, the Fourth Amendment is designed to guard against the government's unfettered use of techniques and technologies that raise the specter of surveillance state.[189] For our forebears, those fears were sparked by broad and indiscriminate use of physically invasive searches and seizures. For contemporary society they are implicated by the pervasive monitoring made possible by aerial drones, GPS-enabled tracking, digital dossiers, and other emerging surveillance technologies. In her concurring opinion in *Jones*, Justice Sotomayor highlighted the democratic consequences of these technologies, which can capture "at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track."[190] As she observed, technologies like GPS and aerial drones "generate[] a precise, comprehensive record of a person's public movements

---

governmental incursion into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."); United States v. White, 401 U.S. 745, 760 (1971) (Douglas, J., dissenting) ("I would stand by *Berger* and *Katz* and reaffirm the need for judicial supervision under the Fourth Amendment of the use of electronic surveillance which, uncontrolled, promises to lead us into a police state."); *Berger*, 388 U.S. at 64 ("[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual . . . indiscriminate used of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments.").

184 460 U.S. 276 (1983),

185 *Id.* at 284. For further discussion of *Knotts*, *see infra* notes 280-295 and accompanying text.

186 *Kyllo*, 533 U.S. at 34.

187 *Id.* at 36.

188 *Id.* at 40.

189 *See* Crocker, *supra* note 154, at

190 132 S.Ct. at 956 (Sotomayor, J., concurring).

that reflect a wealth of detail about her familial, political, professional, religious, and sexual associations."[191] Justice Sotomayor emphasized that people maintain an expectation that the aggregate of these details are generally not subject to governmental monitoring, even if the components are available to public view.[192] She recognized that people rely on quantitative privacy in constructing their identities as citizens and that "[a]wareness that the Government may be watching chills association and expressive freedoms."[193] She therefore concluded that granting law enforcement unfettered access to these technologies "may 'alter the relationship between citizens and government in a way that is inimical to democratic society.'"[194]

As Part II explored, Justice Sotomayor's insights parallel work done in the Information Privacy Law Project, which has long been concerned with the central role played by privacy in democratic societies. Informed by that work, we see strong Fourth Amendment grounds for regulating investigative technologies that are capable of persistent monitoring because they are "inimical to democratic society."[195] Our founders surely knew that there is nothing more threatening to liberty and democracy than a government that exercises control over its citizens' moral commitments and ethical beliefs.[196] They had direct experience with the capacity for unfettered search and seizure to advance the agendas of a tyrannical regime.[197] It therefore comes as no surprise that they embedded in the Bill of Rights not only direct prohibitions on the establishment of religion and the constraint of speech, but also parallel procedural safeguards as well. By itself, and as part of the broader package of protections afforded under the Bill of Rights, the Fourth Amendment therefore plays a critical democracy-preserving role.[198] To the extent a

---

[191] *Id.* at 955.

[192] *Id.* at 955-56. *See also* Maynard at 558.

[193] 132 S.Ct. at 956 (Sotomayor, J., concurring).

[194] *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011). *See also* Crocker, *supra* note 154, at 365, 369.

[195] 132 S.Ct. at 956 (Sotomayor, J., concurring).

[196] *See* United States v. Di Re, 332 U.S. 581, 595 (1948); BREYER, *supra* note 116, at 21; Clancy, *supra* note 158, at 1006-12.

[197] Clancy, *supra* note 158, at 999-1001, 1002-04.

[198] *See White*, 401 U.S. at 762 (Douglas, J., dissenting) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances. Free discourse-a First Amendment value-may be frivolous or serious, humble or defiant, reactionary or revolutionary, profane or in good taste; but it is not free if there is surveillance."); Crocker, *supra* note 154, at 308.

technology threatens unreasonable incursions into spheres, including public ones, linked to projects of self-development, it raises Fourth Amendment concerns.

This result should not change merely because a surveillance technology comes into common use. In holding that thermal detection technology should be subject to Fourth Amendment regulation, Justice Scalia contemplated the possibility that the result might have been different if that technology was in "common public use."[199] The implication is that, if a technology is in common public use, then it is unreasonable, as a descriptive matter, for anyone to expect that they are not being observed with that technology by fellow citizens, and therefore also unreasonable, as a normative matter, to expect that law enforcement officers are not watching using the same technology. This is technological determinism run amok. As Justice Scalia argued, "the power of technology to shrink the realm of guaranteed privacy" *must* be limited lest we "permit police technology to erode the privacy guaranteed by the Fourth Amendment."[200] The alternative is to require that citizens "retir[e] to the cellar, cloaking all the windows with thick caulking, turning off the lights and remaining absolutely quiet."[201] When faced with this alternative, "we must ask what we will have saved if we cede significant ground to a bunker mode of existence, retaining only that sliver of privacy that we cannot envision a madman['s] exploiting."[202] To paraphrase one learned member of the bench, we "simply cannot imagine that the drafters of the Fourth Amendment dictated such dark and cloistered lives for citizens."[203]

Information privacy scholarship has provided theoretical and practical justifications for the proposition that we can and should maintain privacy in large quanta of information. The fundamental concerns for liberty and democracy that lie at the heart of this claim have a secure footing in the Fourth Amendment. The next question, then, is how to translate reasonable

---

[199] *Kyllo*, 533 U.S. at 40.

[200] *Id.* at 34. *See also* Amsterdam, *supra* note 161, at 384 ("Fortunately, neither *Katz* nor the fourth amendment asks what we expect of government. They tell us what we should demand of government.").

[201] Amsterdam, *supra* note 161, at 402

[202] Hutchins, *supra* note, at 464.

[203] Palmieri v. Lynch, 392 F.3d 73, 97 (2d Cir. 2004) (Straub, J., dissenting). *See also* Crocker, *supra* note 154, at 369 ("placing pressure on persons to return to their individual 'private' worlds to seek refuge from government searches and surveillance diminishes the public sphere's security."); Amsterdam, *supra* note 161, at 402 ("This much withdrawal is not required in order to claim the benefit of the amendment because, if it were, the amendment's benefit would be too stingy to preserve the kind of open society to which we are committed and in which the amendment is supposed to function.").

expectations of quantitative privacy into practice. Here again, we take guidance from the Information Privacy Law Project.

IV. THE TECHNOLOGY-CENTERED APPROACH TO PROTECTING QUANTITATIVE PRIVACY

Fourth Amendment debates about quantitative privacy have so far been dominated by discussion of the "mosaic" theory.[204] Under a mosaic approach, Fourth Amendment interests would be determined on a case-by-case basis by assessing the quality and quantity of information about a suspect that law enforcement gathered in the course of a specific investigation.[205] The United States Court of Appeals adopted this approach in the predecessor to *Jones*.[206] Prominent quantitative privacy advocates have since come forward to expand, explore, and defend the mosaic approach.[207] At the same time, the mosaic approach has been a target for pointed criticism on both doctrinal and practical grounds.[208] Although we are not fully persuaded by these criticisms, we nevertheless take a different tack. Taking guidance from the Information Privacy Law Project, we recommend a technology-centered approach to identifying and defending Fourth Amendment interests in quantitative privacy. Parts II and III described the doctrinal foundations for this approach. Here, and in Part V, we address the practicalities.

Beginning in the 1970s, federal and state policymakers adopted measures to protect the privacy of personal information collected by select public and private entities. Their insights have lessons for courts seeking to protect Fourth Amendment interests in quantitative privacy.[209] Most importantly for our purposes, these legislative and policy responses focused on the potential for

---

[204] *See, e.g.*, *Jones*, 132 S.Ct. at 953-54; Kerr, *supra* note 7, at 23-47; Slobogin, *supra* note 20, at 3.

[205] *See, e.g.*, Slobogin, *supra* note 20, at 3.

[206] *See Maynard*, 615 F.3d at 562 .

[207] *See, e.g.*, Slobogin, *supra* note 20, at 3, 12-23.

[208] *See, e.g.*, *Jones*, 132 S.Ct. at 953-54; Kerr, *supra* note 7, at 23-47.

[209] Before going further, an important disclaimer is in order. One of us has previously lamented information privacy law's deficits, including its failure to regulate certain aspects of the information economy. *See* Citron, *Government 2.0*, *supra* note 133, at 838-39 (highlighting failure of federal Privacy Act of 1974 to cover government's collection of social media information through Government 2.0 sites); Citron, *Reservoirs*, *supra* note 101, at 255-61 (exploring state and federal law's failure to protect against leaking of sensitive personal data from private sector databases, especially data brokers); Citron & Pasquale, *supra* note 113, at 1461-63 (discussing regulatory arbitrage responsible for regulatory gaps in privacy protections over governmental surveillance by fusion centers); Citron, *Mainstreaming*, *supra* note 147, at 1826-28 (exploring inadequacies of tort privacy to address information age privacy problems); Posting of Danielle Citron to Concurring Opinions Blog, "Big Data Brokers as Fiduciaries," http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html (critiquing notice and choice regulatory regimes).

abuse inherent in various technologies, adopting interventions that seek to limit risks while balancing competing interests. Policymakers' responses to computerized databases offer a useful example.

In 1973, the Secretary of the Department of Health, Education, and Welfare issued a report specifying the privacy concerns raised by computerized collections of personal data and offering a code of "fair information practices" that would provide procedural safeguards against the technology's inherent potential for abuse.[210] Most entities using large computerized databases of personal data have a natural and understandable interest in maintaining secrecy—to protect their investment and security among other reasons.[211] At the same time, those whose information is aggregated have a natural interest in knowing what personal information is being held, under what terms, and whether it is accurate. After much debate, the Privacy Act of 1974 ("Privacy Act") favored the interests of subjects and prohibited federal agencies from maintaining secret systems of personal records.[212] In a further effort to limit the dangers of secrecy, fair information practices usually guarantee to individuals the right to access their records in order to evaluate, challenge, and correct inaccuracies.[213] Many state and federal laws include this requirement, including the Privacy Act[214] and the Fair Credit Reporting Act of 1970.[215]

Another potential for abuse that attaches to computer databases is the inappropriate collection, use, or disclosure of personal information.[216] As a consequence, statutory responses routinely set limits on the information that certain entities can collect by focusing on what is

---

[210] REGAN, *supra* note 12, at 76.

[211] OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 223 (1993).

[212] 5 U.S.C. § 552a (2006) (regulating federal government agencies' collection, use, and disclosure of personal information).

[213] GANDY, *supra* note 211, at 224. Professor Gandy rightly notes the limits of such individual empowerment—most people have no idea that their personal information appears in thousands upon thousands of digital files, and they become aware only when a problem arises, such as their inability to fly or a denial of credit. *Id.*

[214] 5 U.S.C. § 552a(d) (2006). In its March 2012 recommendations, the Federal Trade Commission urged Congress to pass legislation that would provide consumers with access to information about them held by data brokers so that they could contest inaccuracies. FEDERAL TRADE COMMISSION REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 14 (March 2012).

[215] 15 U.S.C. § 1681a-t (2000) (regulating the collection, use, and sharing of credit information).

[216] GANDY, *supra* note 211, at 223-24. Use restrictions often involve banning the "secondary use" of personal data, by which we mean using data for purposes other than that for which it was originally collected. SOLOVE, UNDERSTANDING, *supra* note 100, at 117-65; REGAN, *supra* note 12, at 76. They may also forbid use of personal information in certain contexts. Consider the Genetic Information Non-Discrimination Act of 2008, which forbids employers and insurers from using confidential genetic data. Disclosure limitations include the prohibition of the sale of certain information without individuals' opt-in consent, such as the Driver's Privacy Protection Act. 18 U.S.C. §§ 2721-2725 (2000).

necessary and proper in light of that entity's role and legitimate needs.[217] For instance, the Privacy Act forbids agencies from amassing personal information without a proper purpose.[218] Many information privacy laws also require opt-in consent. The Children's Online Privacy Protection Act of 1998 (COPPA) essentially bans commercial websites directed at children under thirteen from collecting information directly from youth without a parent or guardian's verifiable knowledge and consent.[219] As Anita Allen explains, under COPPA, parents are "ascribed a powerful right to veto primary collection, primary use, secondary use, and even maintenance of data."[220] More recently, "Do Not Track" legislative proposals would require opt-in consumer before permitting the collection of web browsing data.[221]

In keeping with these policy and legislative models, courts have also taken a technology-centered approach when met with cases involving information government databases. For example, in *United States Department of Justice v. Reporters Committee for Freedom of Press*,[222] the Supreme Court was asked to determine the reach of Freedom of Information Act (FOIA) exemption 7(c), which prohibits federal disclosure of "records or information compiled for law enforcement purposes" that could "reasonably be expected to constitute an unwarranted invasion of personal privacy."[223] The Court held that the exemption prohibited disclosure of FBI "rap sheets" to the media even

---

[217] GANDY, *supra* note 211, at 223.

[218] 5 U.S.C. § 552a(e)(1) (2006) ("agencies shall maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.). The Privacy Act was passed out of concern over "the impact of computer data banks on individual privacy." H.R.REP. NO. 93-1416, p. 7 (1974).

[219] 15 U.S.C. § 6501-506 (Supp. V 2000). In response to COPPA, social network sites like Facebook only permit users who are 13 and up—obtaining verifiable parental consent is both costly and risky if entities learn that parental consent is not valid as the Federal Trade Commission has enforcement power over COPPA violations. ALLEN, *supra* note 128, at 179 (discussing FTC's enforcement actions for COPPA violations). Nonetheless, as social media scholar Danah Boyd and her colleagues have shown, parents routinely assist young children in lying to social network sites like Facebook so that their children can use their services, in some sense turning the purpose of the statute on its head. Danah Boyd et al., "Why Parents Help their Children Lie to Facebook About their Age," FIRST MONDAY, volume 16, Nov. 2011, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075; Posting of Danielle Citron to Concurring Opinions, "Parents Facilitating Facebook Use for Those Under 13: The False Promise of Minimum Age Requirements," Nov. 11, 2011, http://www.concurringopinions.com/archives/2011/11/parents-facilitating-facebook-use-for-the-under-13-set-the-false-promise-of-minimum-age-requirements.html.

[220] ALLEN, *supra* note 128, at 178.

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

[222] 489 U.S. 749 (1989).

[223] 5 U.S.C. 552(b)(7)(C).

though these records are compiled from information in public records.[224] As the Court found, "the fact that 'an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information.'"[225]

Further elaborating the conceptual and practical contours of a technology-centered approach, the Court's reasoning in *Reporters Committee* focused on the change wrought by the expanding capacity of database technology to aggregate and store mass quantities of personal data. As the Court explained, "the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private."[226] The Court further found that computerized compilations of "hard-to-obtain" information in public records "alters the privacy interest implicated by the disclosure of that information."[227] The Court saw "a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[228] The privacy interest in criminal rap sheets was deemed "substantial" because "in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded."[229] According to the Court, the "privacy interest in maintaining the *practical obscurity* of rap-sheet information will always be high."[230] The Court therefore refused to permit the disclosure of the rap sheet because it shed little light on government's inner workings—the core purpose of FOIA—while invading a substantial quantitative privacy interest.[231]

We think that this general technology-based approach is the most sensible and coherent way to understand and protect Fourth Amendment interests in quantitative privacy. As Parts II and III argued, the threshold question on this approach is whether an investigative technique or technology

---

[224] *Reporters Committee*, 489 U.S. at 767.

[225] *Id.* at 770.

[226] *Id.* at 763.

[227] *Id.* at 764.

[228] *Id.*

[229] *Id.* at 771.

[230] *Id.* (emphasis added); see also Woodrow Hartzog and Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. (forthcoming 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597745 (importing the notion of practical obscurity from *Reporters* to the private collection of online personal data).

[231] *Reporters Committee*, 489 U.S. at 773.

has the capacity to facilitate broad programs of indiscriminate surveillance.[232] If it does, then granting law enforcement unfettered access to that technology would threaten "the people's" reasonable expectations of privacy by raising the specter of a surveillance state. As with any other "search," use of the technology would therefore be subject to the crucible of Fourth Amendment reasonableness.

As experience with information privacy law and scholarship suggests, limiting access on a technology-by-technology basis has two important salutary functions. First, it secures generally held expectations of quantitative privacy by limiting law enforcement access to invasive surveillance technologies. Take as examples the aerial drone and GPS-enabled tracking technology officers proposed to use in our hypothetical Stringer Bell case. As we discussed in Part III, most of us maintain a reasonable expectation that our movements in public are not subject to constant governmental surveillance. Both aerial drones and GPS-enabled tracking technologies are precise and highly scalable. GPS technology is also cheap and widely available. Aerial drones are less so, but on their way. These features make GPS technology and aerial drones well suited to broad programs of indiscriminate surveillance. Granting law enforcement unfettered access to these technologies therefore threatens reasonable expectations because it raises the specter of a surveillance state. Once the Court so holds, however, any use of GPS-enabled tracking devices or aerial drones would be treated as a "search." The primary consequence of that status would be to limit access, thereby preserving our reasonable expectations that government agents are not monitoring our every coming and going.

The second benefit of a technology-centered approach is that it maximizes investigative utility while minimizing risks for abuse. Denying law enforcement unfettered access to an investigative technology is not to deny all access. Rather, what is prohibited is "unreasonable" use. Consistent with the calculus of interests evident in the Privacy Act's data collection and use limitations, assessing Fourth Amendment reasonableness requires balancing the needs of law enforcement and the privacy interests of citizens.[233] Applying this balancing test as part of a technology-centered approach to quantitative privacy promises to maximize investigative utility while minimizing risks for abuse. Experience with wiretapping technology provides a useful model.

---

[232] *See* Freiwald, *supra* note 13, at 18-21.

[233] *See* Richards v. Wisconsin, 520 U.S. 385 (1997); Freiwald, *supra* note 13, at 3-4.

Wiretapping technology is, of course, capable of effecting broad programs of indiscriminate surveillance. To protect reasonable expectations that government agents are not listening every time we talk on the phone while meeting the reasonable needs of law enforcement,[234] Congress acted in the shadow of the Fourth Amendment to pass Title III and the Electronic Communications Privacy Act (ECPA).[235] Under Title III and the ECPA, courts must approve wiretap orders.[236] Applications must be in writing and provide the identity of the requesting officers, the crime under investigation, a particular description of the "communications sought to be intercepted," and an account of where and how those communications will be intercepted.[237] Orders will only issue where a court determines that there is "probable cause for belief that an individual is committing, has committed, or is about to commit a particular [enumerated] offense;" "probable cause for belief that particular communications concerning that offense will be obtained through such interception;" and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[238] Wiretap orders themselves must be narrowly tailored and time limited.[239] Courts also have the authority to require regular reports during the pendency of a wiretap warrant and to modify the terms as investigations unfold.[240]

This congressionally devised approach has clear application to aerial drones, GPS-enabled tracking, and other technologies that threaten our expectations of quantitative privacy. First, law enforcement must show probable cause to believe that their use of one of these regulated investigative technologies will produce evidence.[241] For example, in our Stringer Bell case, officers might be required to show that, based on their investigation to that point, there is reason to believe that aerial drone surveillance or GPS monitoring will provide evidence that Bell makes regular visits to stash houses or retail locations associated with the drug conspiracy.

---

[234] *See* Gina Marie Stevens & Charles Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, CRS Rep. 7-5700, 98-326, 5 (Dec. 3, 2009) (available at http://www.fas.org/sgp/crs/intel/98-326.pdf).

[235] 92 Stat. 1783, 50 U.S.C. 1801-1862.

[236] *See* 18 U.S.C. §2516(1) & (2).

[237] *See* 18 U.S.C. §2518(1).

[238] *See* 18 U.S.C. §2516(1)(a)-(s) & 2518(3).

[239] *See* 18 U.S.C. §2518(3) & (5).

[240] *See* 18 U.S.C. §2518(6).

[241] *See* Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

Second, courts should strike a balance between the invasive potential of an investigative technology and the needs of law enforcement. This may mean limiting access to investigations of serious offenses or to circumstances where the technology is likely to provide unique service to investigators. Returning to our Bell example, drug conspiracies are serious. Furthermore, aerial drones and GPS would probably be tremendously valuable to investigating officers because these technologies are uniquely well-suited to the kind of surreptitious and continuous monitoring that would be necessary to document Bell's patterns of travel between locations associated with the drug conspiracy.

Third, courts should tailor warrants and exercise appropriate supervisory authority. For example, a court might set limits on when, how, and how long a drone can be deployed or a GPS device monitored. A court might also require that officers take steps to minimize information about innocent third parties that is incidentally gathered by a drone or to periodically confirm that their suspect is still the sole or primary user of any car being tracked by GPS. As in all Fourth Amendment cases, the guiding principle should be to strike a reasonable balance between the investigative needs of law enforcement and the privacy interests of the suspect and society at large.[242]

The alternative to a technology-centered approach is the case-by-case mosaic test, which asks courts to assess the privacy interests in the information aggregated by law enforcement officers during a specific investigation or on a particular target. As critics have pointed out, this case-by-case approach would require courts to engage in difficult and speculative determinations of the nature and degree of privacy interests at stake in the aggregate of a suspect's movements and conduct.[243] This risks enabling judges to apply their own idiosyncratic standards of privacy.[244] As we explore further in Part V, our technology-centered proposal avoids these and other concerns that attach to the mosaic approach.

---

[242] It is no coincidence that this is precisely the approach taken during the investigation of Jones. The investigating officers sought and received a warrant to install and monitor a GPS device on Jones's car. In keeping with habits developed in the wiretapping context, the court set limits on where and when the device could be installed and how long it could be monitored. *See* United States v. Jones, 132 S.Ct. 945, 948-49 (2012).

[243] *See, e.g.*, *Jones*, 132 S.Ct. at 953-54; Kerr, *supra* note 7, at 23-47

[244] *Kyllo*, 533 U.S. at 40.

V. SOME CONCERNS ABOUT QUANTITATIVE PRIVACY IN PRACTICE

Proposals to grant Fourth Amendment protection to quantitative privacy have met with considerable resistance.[245] This Part addresses some of the most salient criticisms. As our discussion shows, these challenges mainly target the "mosaic" theory of quantitative privacy. Among the many advantages of our technology-centered approach is that it mutes or avoids many of these concerns.

A. The Technology-Centered Approach Resolves Practical Complications

Critics contend that recognizing a quantitative dimension to Fourth Amendment privacy creates thorny practical challenges. Among the most nettlesome is drawing lines between quanta of information that implicate reasonable expectations of privacy and those that do not.[246] Justice Scalia levels this charge in *Jones*, pointing out that Justice Alito's concurring opinion does not explain why short-term monitoring is acceptable but "a 4-week investigation is 'surely' too long."[247] Orin Kerr has echoed Justice Scalia's concerns, asking, "How long must the tool be used before the relevant mosaic is created?"[248] Kerr has also expressed reservations about how to parse mosaics that are aggregated using a variety of techniques and technologies.[249] Although these challenges have a surface appeal, a closer look reveals that they do not raise a significant bar against quantitative privacy generally and have no bite at all against our technology-centered approach.

Backing up a bit, worries about line drawing are by no means unique to quantitative privacy. The Fourth Amendment's center of gravity is reasonableness.[250] Assessments of reasonableness are inherently prone to spectrums and nuances, and seldom are amenable to bright line rules and dramatic contrasts.[251] Despite these difficulties, the Court has yet to abandon a constitutional protection simply because it is challenging to enforce. Rather, the Court leaves it to the lower courts to mush through the "factbound morass of reasonableness."[252] There is no reason to think that the

---

[245] *See, e.g.*, *Jones*, 132 S.Ct. at 953-54; Kerr, *supra* note 7, at 23-47.

[246] *See* Slobogin, *supra* note 20, at 6 17.

[247] 132 S.Ct. at 954. We discuss *Knotts* at greater depth below. *See infra* notes 280-295 and accompanying text.

[248] Kerr, *supra* note 7, at 28.

[249] *Id.* at 31.

[250] *See* Akhil Amar, *Terry and the Fourth Amendment First Principles*, 72 ST. JOHN'S L. REV. 1097, 1101 (1998).

[251] *See* Amsterdam, *supra* note 161, at 366-67.

[252] Scott v. Harris, 550 U.S. 372, 383 (2007).

morass is less passable if the reasonableness inquiry is quantitative rather than qualitative, particularly given the role played by the shared doctrinal values described in Parts II and III.

If protecting quantitative privacy interests on a case-by-case basis ultimately proves too great a burden on lower courts, the Supreme Court always has the option to draw bright, if arbitrary, lines. It would not be the first time. Courts struggled for years to decide how long law enforcement could hold arrestees in custody before violating the requirement for a "prompt" post-arrest hearing.[253] The Court responded by drawing a line at 48 hours–not because it was dictated by the Constitution, but because the Court needed to draw a reasonable line somewhere in order to provide practical guidance to lower courts and law enforcement.[254] Similarly, in *Chimel v. California*, the Court excused courts from engaging in case-by-case assessments of reasonableness by granting law enforcement officers a bright-line privilege to conduct searches of arrestees and the area within their immediate reach and control secondary to all lawful arrests.[255] More recently, the Court headed off future line-drawing concerns by establishing a fourteen-day cooling-off period after suspects invoke their Fifth Amendment right to counsel before law enforcement can reinitiate an interrogation.[256] Again, the Constitution did not dictate that choice. The Court simply responded to the practical need to draw a line somewhere that would ensure reasonable protection from police "badgering."[257] In each of these cases, the Court drew admittedly arbitrary lines in order to provide clear guidance for law enforcement officers and lower courts. There is no reason the Court could not follow a similar course in the quantitative privacy context.[258]

At any rate, line-drawing objections are irrelevant if the Court adopts a technology-centered approach. Whereas a case-by-case approach to quantitative privacy requires courts to evaluate the Fourth Amendment interests implicated by individual mosaics, a technology-centered approach

---

[253] Gerstein v. Pugh, 420 U.S. 103 (1975).

[254] McLaughlin v. County of Riverside, 500 U.S. 44, 55-56 (1991).

[255] 395 U.S. 752 (1969). The *Chimel* rule was modified somewhat by *Arizona v. Gant*, which held that law enforcement officers may only conduct a search incident to arrest of a car if the arrestee or a confederate had access to the car at the time of the search. 556 U.S. 332, 351 (2009). Although *Gant* was limited to the car context, the Court's rationale suggests that there may be future modifications to the *Chimel* rule.

[256] Maryland v. Shatzer, 130 S.Ct. 1213, 1223 (2010).

[257] *Id.*

[258] Justice Alito seems sympathetic to this option. *See Jones*, 132 S.Ct. at 964 (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."). Should the Court want to adopt bright-line rules, Christopher Slobogin has offered a detailed proposal. *See* Slobogin, *supra* note 20, at 17-18.

interrogates the potential for abuse *inherent* in a given surveillance technology. As new surveillance technologies come on line, the Court will need to determine whether those technologies have the capacity to facilitate the sorts of broad programs of indiscriminate surveillance that raise constitutional concerns about a surveillance state. If a particular technology does not raise these concerns, then the Fourth Amendment simply does not apply. If it does, then the government will only be allowed to use that technology when it can meet the demands of Fourth Amendment reasonableness. To be sure, assessments of reasonableness–by balancing the interests of law enforcement and citizens–present their own challenges; but they are both familiar and inherent to Fourth Amendment itself. They are also downstream struggles. Under our approach, the upstream question of whether use of a technology constitutes a search at all is answered *as a general matter* for that technology rather than on a case-by-case basis.[259]

Our technology-centered approach also helps to clarify or resolve other practical challenges leveled against quantitative privacy. For example, in *Jones*, Justice Alito argues that, "longer term GPS monitoring in investigations *of most offenses* impinges on expectations of privacy."[260] This suggests that whether an investigative technology constitutes a Fourth Amendment search relates in part to the seriousness of the crime under investigation. As Justice Scalia rightly points out for the majority, "[t]here is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated."[261] As our technology-centered approach makes clear, however, there is simply no argumentative clash here.

Justice Scalia is surely right that the nature of the offense being investigated has no relevance to the upstream question of whether law enforcement conduct constitutes a "search." Citizens do not possess greater expectations of privacy in less serious crimes. The seriousness of an offense is highly relevant to the downstream question whether a search is "reasonable," however.[262] As we pointed out in Part IV, assessing Fourth Amendment reasonableness is a matter of balancing citizen interests with those of law enforcement. Law enforcement naturally has a weightier interest in

---

[259] For the same reason, our technology-centered approach avoids problems relating to human-collected surveillance mosaics collected via multiple investigative tools and methods. For reasons described below, human surveillance is a not a technology that implicates quantitative privacy.

[260] 132 S. Ct. at 964 (Alito, J., concurring).

[261] *Id.* at 954.

[262] *Cf.* 18 U.S.C. §2516(1)(a)-(s) (limiting use of wiretapping technology to investigations of enumerated offenses).

detecting and prosecuting more serious crimes than it does for minor offenses.[263] When weighing the reasonableness of a search, the seriousness of the offense being investigated is therefore relevant.[264] Likewise, courts can, and should, consider the seriousness of the offense being investigated as a factor when determining whether law enforcement officers acted reasonably during a search or seizure.[265] Thus, although Justice Scalia rightly points out that nature of the offense under investigation is not relevant to the upstream "search" question, good ground exists under our technology-centered approach to recognize that the nature of the offense being investigated bears relevance to downstream reasonableness inquiries.

Our technology-centered approach also helps resolve questions about how a quantitative approach to the Fourth Amendment can be reconciled with the warrant requirement, the probable cause standard, and the particularity requirement.[266] Without predetermining the matter, we suspect that most technologies that raise the specter of a surveillance state will pose sufficiently serious concerns that the warrant clause would apply.[267] As to the mechanics of warrant applications, the lessons learned in the context of government wiretapping, which we discussed in Part IV, have

---

[263] *See* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1 (2011) ("The public's interest in any search or seizure surely depends to some degree on the seriousness of the crime under investigation."); William J. Stuntz, *Commentary, O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 870, 875 (2001) ("A large factor in government need—perhaps the largest—is the crime the government is investigating . . . the worst crimes are the most important ones to solve, the ones worth paying the largest price in intrusions on citizens' liberty and privacy.").

[264] *See New Jersey v. T.L.O.*, 469 U.S. 325, 380 (1985) (Stevens, J., concurring and dissenting in part) ("The logic of distinguishing between minor and serious offenses in evaluating the reasonableness of school searches is almost too clear for argument."); Welsh v. Wisconsin, 466 U.S. 740 (1984) ("Our hesitation in finding exigent circumstances, especially when warrantless arrests in the home are at issue, is particularly appropriate when the underlying offense for which there is probable cause to arrest is relatively minor."); McDonald v. United States, 335 U.S. 451, 459-60 (1948) (Jackson, J., concurring) ("Whether there is reasonable necessity for a search without waiting to obtain a warrant certainly depends somewhat upon the gravity of the offense thought to be in progress as well as the hazards of the method of attempting to reach it."); United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984) ("But maybe in dealing with so intrusive a technique as television surveillance, other methods of control as well, such as banning the technique outright from use in the home in connection with minor crimes, will be required, in order to strike a proper balance between public safety and personal privacy."); Christopher Slobogin, *The World Without the Fourth Amendment*, 39 UCLA L. REV. 1, 68-75 (1991).

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

[266] *See* Kerr, *supra* note 7, at 3, 9.

[267] *See* Hutchins, *supra* note 1, at 460-61 (arguing that GPS-enabled tracking should be subject to the warrant requirement).

obvious application and provide law enforcement and courts with considerable doctrinal guidance.[268] We see no reason to think that warrant applications for aerial drone surveillance, GPS-enabled tracking, or any other pervasive monitoring technology, will pose any intractable new challenges for trial courts.

In his defense of the mosaic approach, Christopher Slobogin has proposed another strategy for avoiding many of these practical concerns.[269] Under his proposal, law enforcement would have unfettered access to even the most invasive investigative technologies and methods as long it was used only for twenty minutes in the aggregate.[270] From twenty minutes to forty-eight hours, he would require a court order.[271] After forty-eight hours officers would need a warrant.[272] The problem with this approach is precisely that it grants law enforcement unfettered discretion to use invasive technologies. In our view, a surveillance state accomplished in short stints is no less oppressive than one produced by long, languorous sweeps. Even if only for a short period of time, or in limited intermittent bursts, affording law enforcement open access to invasive surveillance technologies preserves the possibility that, at any given time, the government is watching each of us or all of us.[273] Although broad, continuous, and indiscriminate monitoring is probably more dangerous for our democracy, the stealth threat of invasive short-term monitoring is nearly as damaging and equally tyrannical. Moreover, as we argued in Parts II and III, the risks to privacy posed by invasive surveillance technologies lie not only with their actual use, but in the ambient potential for their use as well.[274]

B. The Technology-Centered Approach Does Not Implicate Human Surveillance

Another objection to quantitative accounts of Fourth Amendment privacy is that it threatens to limit the range of investigative methods and techniques that have not traditionally been

---

[268] *See supra* notes 234-242 and accompanying text.

[269] *See* Slobogin, *supra* note 20, at 17-18 (defending unfettered access to surveillance technology for twenty minutes).

[270] *Id.* at 17.

[271] *Id.*

[272] *Id.*

[273] This danger is limited somewhat as a practical matter by Slobogin's proposal that the twenty-minute and forty-eight hour thresholds could be met by aggregate use of multiple techniques and technologies. *Id.* Thus, for most investigations officers are likely to burn their twenty-minutes of free access on traditional techniques, and therefore would be obliged to seek a court order before using surveillance technology. The people most likely to benefit from this practical security are, of course, criminals or others who know they are targets of an investigation. For the vast majority of us, innocence would actually enhance our sense of vulnerability to surveillance.

[274] *See supra* notes 133-143 and accompanying text.

considered searches. The most commonly cited example is human surveillance. For example, Orin Kerr has wondered whether "visual surveillance [should] be subject to mosaic analysis."[275] Justice Scalia also expressed concern about this possibility in his majority opinion in *Jones*.[276] Adding weight to their fears, Christopher Slobogin, a mosaic theory advocate, has argued that human surveillance should be subject to the same Fourth Amendment regulation as GPS-enabled tracking.[277]

Our technology-centered approach to quantitative privacy would not implicate human surveillance and other traditional investigative techniques. As Justice Alito observed in *Jones*, "[t]raditional [human] surveillance for any extended period of time [is] difficult and costly and therefore rarely undertaken."[278] Human surveillance is therefore incapable of sustaining the sort of broad, continuous, and indiscriminate surveillance that is characteristic of a surveillance state. This has been true in the past and remains true today. Under a technology-centered approach to quantitative privacy, human surveillance would therefore not warrant Fourth Amendment review unless something radical changed about those practical limitations. The result would not change even if law enforcement could aggregate a detailed mosaic about an individual's activities using multiple traditional law enforcement methods, so long as none of them was subject to Fourth Amendment restraint by the standards of the technology-centered approach.[279]

C. The Technology-Centered Approach Does Not Violate Stare Decisis

Another potential bar to judicial recognition of quantitative privacy is stare decisis and particularly *United States v. Knotts*.[280] In *Knotts*, the Court held that using a beeper device to track a suspect's car on public streets did not constitute a "search" because the suspect lacked a reasonable expectation of privacy in his public movements.[281] The parallel between *Knotts* and *Jones* is obvious. In both cases, law enforcement officers used a passive signaling device attached to a car. In both cases, the devices revealed only movements on public streets. In both cases, those movements were

---

[275] Kerr, supra note 7, at 30.

[276] 132 S.Ct. at 953-54.

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

[278] 132 S. Ct. at 963 (Alito, J., concurring).

[279] Thus, our technology-based approach also answers Orin Kerr's concerns about how quantitative privacy would apply to bodies of information aggregated by different law enforcement groups or agencies. *See* Kerr, *supr*a note 7, at 31.

[280] 460 U.S. 276 (1983).

[281] *Id.*

exposed to public view. Given these parallels, *Knotts* would seem to control cases like *Jones*, thus barring Fourth Amendment review of GPS-enabled tracking so long as the technology is only used to monitor movements in public.[282] The result would not seem to change if the technology at stake was aerial drones. Should the Court eventually adopted the views expressed by the *Jones* concurrences, it therefore seems obliged to overrule *Knotts*.

Our technology-centered approach avoids this entanglement with stare decisis by providing easy grounds for distinguishing *Knotts* from cases that involve GPS-enabled tracking or other advanced surveillance technology like aerial drones.[283] The beeper technology used in *Knotts* was simply incapable of pervasive surveillance. It could only provide directional information, not a suspect's precise location.[284] To be of any use at all, the beepers used in *Knotts* needed to be in close proximity to a dedicated radio receiver.[285] Because no stable network of these receivers existed, officers had to follow the beepers, and hence the suspects, to track them.[286] This beeper technology was thus little more than an adjunct to traditional surveillance and therefore labored under the same practical limitations.[287] That is why the *Knotts* Court ultimately held that the beeper technology used in that case "raise[d] no constitutional issues which visual surveillance would not also raise."[288]

The GPS-enabled tracking technology used in *Jones* is materially different.[289] It therefore implicates markedly "different constitutional principles."[290] Like many twenty-first century surveillance technologies–including aerial drones– GPS is precise and highly scalable. Its unfettered use implicates risks of broad, continuous, and indiscriminate surveillance. GPS technology provides second-by-second location data. Due to the nearly ubiquitous reach of satellite networks, GPS technology has extensive range and can locate devices within a range of several feet.[291] Unlike

---

[282] Would have to be public movements. *See* United States v. Karo, 468 U.S. 705, 713-14 (1984).

[283] *See Jones*, 132 S.Ct. at 954.

[284] With a stable network of receivers, officers might have been able to triangulate Knotts's position. Cellular phone providers presently can locate subscribers' phones using this same technique. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 677, 679 (2011).

[285] *Knotts*, 460 U.S. at 278.

[286] *Id.*

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

[288] *Knotts*, 460 U.S. at 285.

[289] *See* Hutchins, *supra* note 1, at 414-21.

[290] *Knotts*, 460 U.S. at 284.

[291] *See* Hutchins, *supra* note 1, at 418-20.

beeper technology of the past, GPS-enabled tracking devices gather location data without any need for human beings to "tail" targets.[292] Officers can watch the GPS device's precise movements from anywhere or just let a computer do the work for them.[293] GPS networks can cheaply track millions of devices, and algorithms can search unlimited hours of location data.[294] By its very nature, then, GPS technology raises the specter of a surveillance state.[295] The constitutional distinction between *Knotts* and *Jones* is therefore not that officers exercised constraint in their use of technology in *Knotts*, but, rather, that the technology used in *Knotts* came with inherent constraints that do not bedevil many of today's new and developing surveillance technologies.

Another potential stare decisis challenge to quantitative privacy is the third-party doctrine. The Court has long held that, although the Fourth Amendment limits the conduct of state agents, it does not apply to private citizens.[296] Under this third-party doctrine, citizens who share information with others assume the risk that what they share might be passed along to law enforcement.[297] There is therefore no Fourth Amendment violation if a bank shares a customer's financial records with law enforcement[298] or if a telephone company discloses records of phone calls customers made or received.[299]

---

[292] Michael Ferraresi, "GPS Makes Police Officers' Job Easier, Safer," ARIZONA REPUBLIC, Oct. 7, 2005, http://www.azcentral.com/community/scottsdale/articles/1007sr-technology07Z8.html; see alsohttp://www.gps.gov/systems/gps/performance/accuracy/.

[293] Carrie Johnson and Steve Inskeep, "GPS Devices Do the Work of Law Enforcement," NATIONAL PUBLIC RADIO, October 27, 2010, http://www.npr.org/templates/story/story.php?storyId=130851849

294 *See* Slobogin, *supra* note 20, at 2; Erik Eckholm, *Private Snoops Find GPS Trail Legal to Follow*, N.Y. TIMES, Jan. 28, 2012 (reporting that sales of GPS-enabled tracking devices surpass 100,000 a year and are rising); Ben Hubbard, "Police Turn to Secret Weapon: GPS Device," WASH. POST, A1 (Aug. 13, 2008), available at http://www.washingtonpost.com/wpdyn/content/article/2008/08/12/AR2008081203275.html?nav=rss_metro/va.

[295] Hutchins, *supra* note 1, at 421.

[296] *See, e.g.*, Burdeau v. McDowell, 256 U.S. 465 (1921).

[297] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (a citizen "takes the risk, in revealing his affairs to another, that the information will be conveyed by the person to the government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

[298] California Banker's Assoc. v. Shultz, 416 U.S. 21 (1974). Congress responded to decisions like *Miller* and *Schultz* by passing the Right to Financial Privacy Act of 1978, 29 U.S.C. §§ 3401-22, which provides bank customers some privacy regarding their records held by banks and other financial institutions and stipulates procedures whereby federal agencies can gain access to those records.

[299] Smith v. Maryland, 442 U.S. 735, 744 (1979) ("a person who uses the phone . . . assume[s] the risk that the [telephone] company would reveal to the police the numbers he dialed."). The Pen Register Act attempted to fill the void left by *Smith v. Maryland* by requiring a court order to use a pen register or trap and trace device. 18 U.S.C. § 3121(a). Whereas a pen register records the telephone numbers someone dials from a home, a trap and trace device creates a list of the telephone numbers of incoming calls. SOLOVE, DIGITAL PERSON, *supra* note 100, at 205.

Quantitative privacy concerns implicate the third-party doctrine because vast reservoirs of our private data reside in the hands of private entities.[300] GPS chips in telephones, cars, or computers share a steady stream of information about our movements with companies providing services associated with these devices. Internet Service Providers and search engines log where we go and what we do online. Credit card companies record our shopping habits. Data brokers collect and mine a mind-boggling array of data about us, including Social Security numbers, property records, public-health data, criminal justice sources, car rentals, credit reports, postal and shipping records, utility bills, gaming, insurance claims, divorce records, online musings, browsing habits culled by behavioral advertisers, and the gold mine of drug- and food-store records.[301] Under the third-party doctrine, the government appears to have unfettered access to these reservoirs of personal information.[302] Thus, Chris Hoofnagle has dubbed data brokers "Big Brother's Little Helpers."[303]

In her concurring opinion in *Jones*, Justice Sotomayor suggests that recognizing a constitutional dimension to quantitative privacy might require "reconsider[ing] the premise that an individual has no reasonable expectations of privacy in information voluntarily disclosed to third parties."[304] Otherwise, the government's ability to aggregate and exploit privately collected information would be unfettered. This would of course entail radical changes to a substantial body of Fourth Amendment law surrounding the third-party doctrine.

Our technology-based approach suggests that dramatic changes to the third-party doctrine may not be necessary. That is because when a private entity acts as a state agent, the Fourth Amendment applies with full force.[305] The traditional test for determining whether a non-state entity acts as a state agent focuses on whether that entity was directed or incentivized by the government, whether it believed it was acting on state authority, or whether a government agent knew or had reason to know that the private entity was acting to advance state goals.[306] We suspect

---

[300] *See* Slobogin, *supra* note 20, at 7.

[301] Citron, *Reservoirs*, supra note 101, at 1451; Posting of Danielle Citron to Concurring Opinions Blog, "Big Data Brokers as Fiduciaries," http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html

[302] Citron & Pasquale, *supra* note 113, at 1451.

[303] Hoofnagle, *supra* note 101, at 595.

[304] 132 S.Ct. at 957. *See also* Crocker, *supra* note 116 (arguing for a modification of the third-party doctrine). *See also* Crocker, *supra* note 154, at 375.

[305] *See* Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602 (1989).

[306] *Id.*

that in most cases where government leveraging of private data reservoirs would raise quantitative privacy concerns, one or more of these tests of state agency will be satisfied. As a consequence, the crisis for the third-party doctrine that Justice Sotomayor foreshadows is unlikely to occur.

Consider the example of fusion centers described in Part II. Commercial data brokers grant fusion centers access to massive data streams, specifically tailored for government agencies.[307] Private entities enable fusion centers to search their databases for relevant information. For instance, freight operator CSX Transportation gives fusion centers access to its secure online systems, permitting real-time tracking of the company's rail cars, customers, and contents.[308] Arizona's fusion center works "closely with utilities, fuel tank farms, shopping center owners, railroad operators, [and] private security professionals."[309] Non-disclosure agreements facilitate information-sharing arrangements with private entities.[310] With this level of government engagement, there is little doubt that the private entities who participate in fusion centers are acting as state agents. The result would be the same for companies like Google or Amazon if they are routinely the subject of government subpoenas. Albeit unwillingly, these kinds of repeat players function as state agents when they gather and aggregate personal information.

Where the state agent doctrine is inadequate, experience with the Information Privacy Law Project suggests that legislation has the potential to fill in the gaps.[311] Ongoing efforts to legislate on the state and federal level represent important and promising opportunities to limit non-state actors. For example, Congress has stepped in with laws that protect personal data entrusted to third parties like banks and telephone companies.[312] This is not to say that Congress has done a perfect job.[313] Nevertheless, its past and continuing efforts to regulate private entities that collect and store

---

[307] Citron & Pasquale, *supra* note 113, at 1451-53; Hoofnagle, *supra* note 101, at 595-97.

[308] Alice Lipowicz, *CSX to Share Data with Kentucky Fusion Center*, WASH. TECH. (Aug. 2, 2007), http://washingtontechnology.com/articles/2007/08/02/csx-to-share-data-with-kentucky-fusion-center.aspx?sc_lang=en.

[309] Joseph Straw, *State Perspective—Artizona*, SECURITY MGMT. (Jan. 1, 2007), http://www.securitymanagement.com/article/state-perspective-arizona.

[310] *Focus on Fusion Centers: A Progress Report, Hearing Before the Ad Hoc Subcomm. on State, Local, and Private Sector Preparedness and Integration of the S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 35 (2008).

[311] *See supra* notes 209-244 and accompanying text.

[312] SOLOVE, DIGITAL PERSON, *supra* note 100, at 202-08 (discussing various legislative regimes regulating government access to third party records that were passed in response to the Supreme Court's refusal to find the Fourth Amendment applicable); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 905, 931-39 (2009) (discussing state privacy legislation).

[313] SOLOVE, NOTHING TO HIDE, *supra* note, at 165.

personal information suggest that there is no immediate crisis that would require abandoning the third-party doctrine.[314] Less so still if courts begin to take seriously the close agency relationships that many private entities have developed with the government.

CONCLUSION

Recognizing a constitutional interest in quantitative privacy buttresses Fourth Amendment defenses against a surveillance state. Until now, practical limitations inherent to many investigative techniques, cultural constraints on mutual surveillance, and existing Fourth Amendment doctrines have provided a virtual guarantee that traditional investigative techniques would not produce the kind of continuous and indiscriminate monitoring that raises the specter of a surveillance state.[315] There simply are not enough police officers to follow all of us all of the time. As a society, we have stalwartly resisted the temptations of mutual surveillance that sustained many totalitarian states. Finally, Fourth Amendment doctrine has preserved an archipelago of safe spaces and activities beyond the gaze of government agents. As a consequence, we have sustained a fairly stable balance between government power and private citizenship that allows us to pursue projects of self-development free from fear that the government is watching.[316]

Recent technological developments, such as GPS-enabled tracking, digital monitoring, and domestically deployed drones, threaten to alter this balance. By nature, these technologies make continuous monitoring of anyone and the indiscriminate monitoring of everyone possible. Granting the government unfettered access to these technologies is what opens the door to a surveillance state and the tyranny it entails. It is therefore at the point of unfettered access to those technologies that Fourth Amendment concerns attach under our technology-centered approach to quantitative privacy.

---

[314] For example, on August 1, 2012, Representative Ed Markey, co-chair of the Bipartisan Congressional Privacy Caucus, released a draft of the Drone Aircraft Privacy and Transparency Act of 2012, which would require police to get a warrant to conduct surveillance using drones and tighten regulations on the kind of data government and private companies can collect. http://www.scribd.com/doc/101745377/Drones-Legislation.

[315] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

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