CHICAGO

COASE-SANDOR INSTITUTE FOR LAW AND ECONOMICS WORKING PAPER NO. 727
PUBLIC LAW AND LEGAL THEORY WORKING PAPER NO. 534

COASE-SANDOR INSTITUTE
FOR LAW AND ECONOMICS
THE UNIVERSITY OF CHICAGO LAW SCHOOL

# ACTUAL EXPECTATIONS OF PRIVACY, FOURTH AMENDMENT DOCTRINE, AND THE MOSAIC THEORY

*Matthew B. Kugler & Lior Strahilevitz*

THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

November 2015

MATTHEW B. KUGLER AND
LIOR JACOB STRAHILEVITZ

# ACTUAL EXPECTATIONS OF PRIVACY, FOURTH AMENDMENT DOCTRINE, AND THE MOSAIC THEORY

The mosaic theory of the Fourth Amendment holds that, when it comes to people's reasonable expectations of privacy, the whole is greater than the sum of its parts.[1] More precisely, it suggests that the government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic. This insight, that the incremental privacy threat posed by the government's acquisition of information increases as more information is obtained, was given its most forceful articulation by

Matthew B. Kugler is Assistant Professor, Northwestern University Pritzker School of Law. Lior Jacob Strahilevitz is Sidley Austin Professor of Law, University of Chicago.

Authors' note: The authors thank Katerina Linos, Eric Oliver, and Peter Winn for helpful discussions; Adam Chilton, Paul Crane, Adam Feibelman, Lee Fennell, Barry Friedman, Jancy Hoeffel, Chris Hoofnagle, Orin Kerr, Richard McAdams, Pamela Metzger, Paul Ohm, Eric Posner, Richard Posner, John Rappaport, Richard Re, Christopher Slobogin, Geoffrey Stone, Matt Tokson, Heather Whitney, and Tal Zarsky; workshop participants at Tulane Law School, the University of Chicago Law School, Boston University Law School, UCLA Law School, and Emory Law School for constructive comments on earlier drafts; Michelle Hayner and Adam Woffinden for research assistance; plus the Russell J. Parsons and Bernard Sang Faculty Research Funds and the Coase-Sandor Institute for Law & Economics for generous research support.

[1] *United States v Maynard*, 615 F3d 544, 558 (DC Cir 2010) ("[T]he whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than the sum of its parts.").


978-0-226-39221-9/2016/2015-0006$10.00

Judge Douglas Ginsburg of the D.C. Circuit in the landmark case that ultimately became *United States v Jones*.[2]

Writing for the Court of Appeals, Judge Ginsburg used a mosaic theory to explain why long-term geolocation surveillance of a vehicle was categorically different from short-term surveillance:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.[3]

This analysis allowed the D.C. Circuit to reach an otherwise difficult conclusion. A controlling precedent, *United States v Knotts*,[4] had held that an individual driving a car on public roads has no expectation of privacy in her whereabouts.[5] Ginsburg nevertheless held that a lack of constitutional protection against being seen in public at any given moment in time does not preclude the possibility that the police would need to obtain a warrant to record someone's movements for several weeks. This approach stood in stark contrast to most prior Fourth Amendment thinking.[6]

Soon thereafter, the Supreme Court granted certiorari and agreed to hear the *Jones* case. The Court decided in favor of the defendant on narrow grounds, holding that the installation of the device was a trespass and therefore a search.[7] To the surprise of many, however, four Justices signed a concurring opinion that embraced much of Judge Ginsburg's mosaic theory.[8] Justice Alito, writing for Justices

---

[2] 132 S Ct 945 (2012).

[3] *Maynard*, 615 F3d at 562.

[4] 460 US 276 (1983).

[5] Id at 281. For an early and incisive critique of *Knotts*, see Richard H. McAdams, Note, *Tying Privacy in Knotts: Beeper Privacy and Collective Fourth Amendment Rights*, 71 Va L Rev 297 (1985).

[6] See David Gray, Danielle Keats Citron, and Liz Clark Rinehart, *Fighting Cybercrime After United States v. Jones*, 103 J Crim L & Criminol 745, 760 (2013).

[7] *Jones*, 132 S Ct at 949.

[8] See, for example, Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law* 334 (Wolters Kluwer, 5th ed 2015) ("Both concurring opinions, involving five justices, embraced

Ginsburg, Breyer, and Kagan, wrote that warrantless geolocation surveillance for four weeks was unconstitutional, even though surveillance for a short period of time would not be. As he stated:

> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. 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.[9]

As we demonstrate below, Justice Alito mostly grounded his short-term versus long-term distinction in the purported actual beliefs of reasonable people, referring in various places to "popular attitudes," "popular expectations," and "the average person's expectations."[10] In her separate concurring opinion, Justice Sotomayor expressed approval of mosaic-theory-style reasoning, focusing on the conclusions that could be drawn from prolonged surveillance.[11] She agreed with Justice Alito that "longer term GPS monitoring in investigations of most offenses" should be deemed a search, though she did not say whether a search warrant should also be required for short-term

---

a new theory of privacy. In previous cases, the Court has focused extensively on whether something . . . was exposed to the public. The concurrences recognize that extensive and aggregated surveillance can violate a reasonable expectation of privacy regardless of whether or not such surveillance occurred in public."); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich L Rev 311, 314 (2012) ("The concurring opinions in *Jones* raise the intriguing possibility that a five-justice majority of the Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection."); but also see note 30 (identifying another possible explanation for the duration distinction).

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

[10] See Part II.A.

[11] *Jones*, 132 S Ct at 955 (Sotomayor, J, concurring) ("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. See, for example, *People v Weaver*, 12 NY3d 433, 441–42 (2009) ('Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on'")); Ryan Birss, Note, *Alito's Way: Application of Justice Alito's Opinion in United States v. Jones to Cell Phone Location Data*, 65 Hastings L J 899, 925 (2014).

geolocation monitoring.[12] In light of Alito's and Sotomayor's opinions, it seems likely that there are now five votes for the mosaic theory and its "duration-sensitive" approach.[13]

Indeed, post-*Jones* cases indicate that nearly all the Justices are beginning to talk about privacy in mosaic-theory terms. *Riley v California*[14] made this particularly clear. Chief Justice Roberts, writing on behalf of eight Justices, held that the police generally could not search an arrestee's cell phone at the time of arrest without first obtaining a warrant. Explaining why the arrestee's wallet could be searched but his cell phone could not, Roberts offered an argument that is much akin to the mosaic theory:

> [A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that *reveal much more in combination than any isolated record*. . . . The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. [Finally], *the data on a phone can date back to the purchase of the phone, or even earlier*. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; *he would not carry a record of all his communications with Mr. Jones for the past several months*, as would routinely be kept on a phone.[15]

It is this aggregation of multifaceted information over a long time period—which is purported to be qualitatively distinct from the mere snapshot exposed by prior searches—that worried the Chief Justice. Because of this emphasis on quantity and time scale, *Riley* hints that mosaic-theory reasoning about the Fourth Amendment may have rapidly won over nearly all the Justices. And Antonin Scalia's unexpected death means that the only Justice who has authored a recent opinion openly skeptical of the mosaic theory is no longer on the Court.[16]

---

[12] *Jones*, 132 S Ct at 955 (Sotomayor, J, concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention.").

[13] See Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn L Rev 407, 507 (2012); Gray et al, 103 J Crim L & Criminol at 764 (cited in note 6); Kerr, 111 Mich L Rev at 313 (cited in note 8); Richard M. Re, *The Due Process Exclusionary Rule*, 127 Harv L Rev 1885, 1963 (2014).

[14] 134 S Ct 2473 (2014).

[15] Id at 2489 (emphasis added).

[16] *Jones*, 132 S Ct at 954 (majority opinion) ("The concurrence posits that 'relatively short-term monitoring of a person's movements on public streets' is okay, but that 'the use of

If embraced by the Court, the mosaic theory would upend decades of settled doctrine.[17] It is therefore hardly surprising that legal scholars have begun to explore a number of important questions posed by the sudden rise of the mosaic theory.[18] But at least one fundamental question remains unaddressed by the courts and in the literature so far: Does the mosaic theory, which is explicitly grounded in people's reasonable expectations of privacy, reflect the public's *actual* expectations? When presented with the kinds of scenarios that the Court was wrestling with in *Jones*—momentary geolocation surveillance, day-long surveillance, month-long surveillance, etc.—do ordinary Americans agree with Justice Alito that duration determines expectations of privacy?

The answer is that the public does not agree with him. Specifically, only a very small proportion of the respondents in our representative (census-weighted) national sample said that the duration of the surveillance affected whether they would expect privacy in their geolocation information. According to our survey data, a large majority of Americans always expect privacy in their geolocation information, a meaningful minority never expect privacy, and only a tiny remnant allow their expectations to depend on surveillance duration. Put another way: If we ask people whether they expect the police to be able to obtain geolocation information track-

longer term GPS monitoring in investigations *of most offenses*' is no good. (emphasis added). That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is 'surely' too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an 'extraordinary offense' which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

[17] See Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 BU L Rev 1809, 1840–44 (2014); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 Cal L Rev 1069, 1072–73 (2014).

[18] See, for example, Bedi, 94 BU L Rev at 1809 (cited in note 17); Jace C. Gatewood, *District of Columbia Jones and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 Neb L Rev 504 (2014); David Gray and Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn L Rev 62 (2013); Gray et al, 103 J Crim L & Criminol at 745 (cited in note 6); Kerr, 111 Mich L Rev at 311 (cited in note 8); Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 Notre Dame L Rev 1733 (2011); Andrew B. Talai, Comment, *Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age*, 102 Cal L Rev 729 (2014).

ing someone's whereabouts over the course of a day or a month, the clear plurality say no to both, a sizable minority say yes to both, and a very small number of respondents provide the answer that is consistent with the mosaic theory and Justice Alito's gloss on it—yes for one day and no for one month. The percentage of respondents who believed that surveillance either definitely or likely violates a reasonable expectation of privacy rose by just *three* percentage points when the surveillance's duration was described as month-long rather than day-long. Following people's actual expectations of privacy would thus require overruling *Knotts* rather than trying to preserve it via the mosaic theory.

That duration was of such limited relevance took us by surprise. We believe it would take at least four Supreme Court Justices by surprise as well. Before we launched our first survey, we had expected that respondents would agree with Justice Alito that the duration of the surveillance was central to the question of whether police surveillance violates a reasonable expectation of privacy. After learning otherwise in Wave 1 of our survey, we supplemented Wave 2 so that respondents who believed that surveillance duration does not matter would be asked follow-up questions to explain their reasoning. Our results here were also surprising. The respondents who consistently felt that surveillance for a day, a week, or a month *did not* violate their reasonable expectations of privacy overwhelmingly embraced the third-party doctrine as the basis for their views.[19] Notwithstanding the criticism to which this doctrine has been subjected in recent years,[20] about 11% of our sample (and 65% of those with low privacy expectations) embraced it and its privacy-skeptical implications. Respondents who felt that both one-day and

[19] The third-party doctrine holds that individuals have no reasonable expectation that information voluntarily shared with third parties (like the bank, a telecommunications company, or passersby) will not be exposed to the government's agents. See, for example, *United States v Miller*, 425 US 435, 443 (1976).

[20] See, for example, Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkeley L & Tech L J 1199 (2009); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepperdine L Rev 975, 976–77 (2007); Erin E. Murphy, *The Case Against the Case for the Third Party Doctrine: A Response to Epstein and Kerr*, 24 Berkeley Tech L J 1239 (2009); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S Cal L Rev 1083, 1089–1117 (2002); Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L Rev 581 (2011); text accompanying note 172. But see Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 Mich L Rev 561 (2009) (defending the doctrine).

one-month surveillance *does* violate their reasonable expectations of privacy were far more numerous but slightly less unified in their rationales. The most commonly expressed bases for this view were (1) that the police are likely to abuse any power to obtain the geolocation of an individual's car,[21] and (2) that giving the police such power threatens personal freedom. Both responses commanded majority support among duration-insensitive respondents who believe the surveillance infringes on reasonable expectations of privacy.[22]

A third wave conducted almost a year later replicated the prior findings, showing an impressive level of stability in privacy expectations over time. This third collection also included separate questions on the perceived *intrusiveness* of searches. Though the doctrine emphasizes expectations in determining whether a law enforcement action implicates the Fourth Amendment, the perceived intrusiveness of a proposed search is relevant to the question of whether a particular privacy expectation is one that society is prepared to recognize as reasonable.[23] More participants drew duration distinctions in the domain of intrusiveness but, again, consistency was the rule.

In this article, we will argue that data about what the public expects (and regards as intrusive) are not only interesting but also doctrinally relevant. We proceed as follows. Part I provides some essential background on Fourth Amendment search and seizure law and then examines the post-*Jones* case law to see how the question of surveillance duration has played out. The lower courts have embraced inconsistent approaches to the question of how to treat the suggestion in Justice Alito's concurrence that warrantless surveillance becomes unconstitutional as its duration increases.

Part II offers several arguments about why drawing on reliable social science research about public sentiment lends itself to relatively predictable and workable rules of thumb for law enforcement and the citizenry to follow. We also parse the case law to suggest a framework that is more coherent than the ones proposed in the

[21] Notably these surveys were conducted in June and July 2014, prior to the prominent controversies surrounding Michael Brown, Eric Garner, and Laquan McDonald capturing public attention.

[22] Respondents were asked to select the one or two rationales that best explained their views. Among those with consistently low privacy expectations, 48.9% selected one option, 37.8% selected two, and the remainder selected three or more. Among those with consistently high expectations, 37.8% selected one option, 39.2% selected two options, and the remainder selected two or more.

[23] See notes 131–32 and accompanying text.

existing doctrinal literature. Under our proposed approach, inquiries concerning the scope of the Fourth Amendment would have a tripartite framework. First, courts would decide whether law enforcement actions violate a suspect's property rights. If so, the police conduct would amount to a search. This is consistent with the Court's opinion in *Jones*, which focused on whether law enforcement had trespassed on the suspect's property by installing a small tracking device on his car. Second, if there is no police trespass, then the courts would apply a clarified version of the framework from *Katz v United States*. *Katz* prong 1 would prompt courts to scrutinize survey research to determine whether people in general expect privacy against a particular law enforcement strategy. Third, *Katz* prong 2 would focus on the sensitivity of the information collected by the police, relying in part on survey research results about whether information revealed by a particular category of searches would be sensitive or embarrassing. Despite the enhanced role of survey research in our framework, the ultimate determination of whether a warrant is required in a given instance would, as now, involve balancing of a variety of costs and benefits. Survey data would help illuminate some of the costs associated with police searches, but there are other costs and benefits that would need to be evaluated using other strategies at the post-*Katz* reasonableness stage. Part II also provides a truncated normative defense of this approach.

Part III presents our empirical data, derived from census-representative surveys. Our main finding is that the duration of surveillance barely affects the extent to which the public regards geolocation tracking as invading their reasonable expectations of privacy. Whatever the policy merits of the mosaic theory, it does not resonate intuitively with ordinary Americans. Our data also indicate that younger Americans actually have stronger expectations of privacy in their geolocation data than older Americans, and that anti-authoritarian attitudes are strongly correlated with privacy expectations. Finally, our data give a clear answer to the question of whether Americans expect that the police will be able to monitor the location of citizens' vehicles remotely, without first obtaining a warrant. Most Americans who take a position regard such warrantless surveillance as a violation of their reasonable expectations of privacy. The rejection of the mosaic theory's duration sensitivity is therefore principally driven by those who have more robust privacy expectations than are accounted for in existing doctrine.

Part III concludes by offering new data on popular expectations regarding a number of presently controversial policing strategies, such as the use of stingray devices to determine citizens' geolocation or the examination of hotel guest registries. By presenting a census-representative sample of the population with various neutral scenarios, it is easy to spot those instances in which police tactics are fully consistent with or largely contrary to prevalent expectations of privacy.

## I. Surveillance Duration After Jones

In 1967, the Supreme Court held that wiretaps are a search under the Fourth Amendment in *Katz v United States*.[24] Nearly half a century later, in 2012, the Court held in *United States v Jones* that month-long geolocation surveillance, effectuated by the installation of a GPS device on a vehicle, similarly amounted to a search.[25] Interestingly, in neither pathbreaking case is the Court's opinion the central focus of scholarly inquiry. Rather, it is the concurring opinions of Justice Harlan in *Katz* and Justice Alito in *Jones* that tantalize jurists and fascinate scholars.

Harlan's concurrence in *Katz* set out the reasonable expectations test for Fourth Amendment protections. He wrote that police conduct amounts to a search, thereby implicating the Fourth Amendment, when "a person [exhibits] an actual (subjective) expectation of privacy, and [when] the expectation [is] one that society is prepared to recognize as 'reasonable.'" In subsequent cases, this test was embraced by the Court as a whole and has become the key touchstone for determining whether any particular form of surveillance constitutes a "search" within the meaning of the Fourth Amendment.[26] Thus, for nearly fifty years courts have spoken of "reasonable expectations of privacy."

---

[24] 389 US 347, 362 (1967); see also Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* 13 (Chicago, 2007) ("*Katz v. United States* [is] the most important judicial decision on the scope of the Fourth Amendment.").

[25] Jones, 132 S Ct at 949.

[26] 389 US 361 (Harlan, J, concurring). Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn L Rev 349, 382 (1974) (describing *Katz* as a "watershed in fourth amendment jurisprudence"). For an illuminating examination of *Katz*'s backstory, see Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 McGeorge L Rev 1 (2009). *The* Katz test is also used to determine whether a defendant's conduct is covered by federal wiretap statutes. See, for example, *Huff v Spaw*, 794 F3d 543, 548 (6th Cir 2015); *United States v Turner*, 209 F3d 1198, 1200 (10th Cir 2000).

Some courts and commentators have treated Justice Alito's opinion in *Jones* as a similarly important shift in Fourth Amendment jurisprudence. His focus on surveillance duration makes the combination of two discrete acts that are independently not searches—say, surveillance for one week and surveillance for the next week—a Fourth Amendment search. One federal court recently dubbed Alito's opinion "the shadow majority opinion in *United States v Jones*,"[27] and academic commentators have similarly referred to it as "*Jones*'s second majority opinion,"[28] invoking Sotomayor's adoption of portions of Alito's reasoning as a justification for adding her vote to Alito's four. After *Jones*, the "vexing problems" raised by Alito's concurrence have become arguably the most important looming questions in Fourth Amendment law.[29] If Justice Alito's apparent[30] nod in the direction of the mosaic theory represents the future of *Katz*, then many settled assumptions about Fourth Amendment search doctrines may be called into question.

Though the Supreme Court has not revisited the issue of surveillance duration in the years since *Jones*, the issue has already arisen in a number of lower court cases. In *United States v Skinner*,[31] for example, the Sixth Circuit considered whether tracking a criminal suspect for three days by pinging his phone to determine the clos-

---

[27] *In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted]*, 40 F Supp 3d 89, 92 (DDC 2014).

[28] Jonathan Siegel and Kate Hadley, *Jones' Second Majority Opinion: Justice Alito's Concurrence and the New Katz Test*, 31 Yale L & Policy Rev Inter Alia 1, 2 (2012) ("While the concurrence only gained four votes in *Jones*, Justice Sotomayor explicitly endorsed Justice Alito's approach in her own concurrence, providing the necessary fifth vote for a future majority opinion.").

[29] See note 16; see generally Caleb Mason, *New Police Surveillance Technologies and the Good-Faith Exception: Warrantless GPS Tracker Evidence after United States v. Jones*, 13 Nev L J 60, 61 (2012).

[30] We say "apparent" here because it is conceivable that Justice Alito and the Justices who signed his concurrence were implicitly adopting another rationale for their duration-sensitive shadow holding. Perhaps they believe that because law enforcement have long been able to tail suspects for a day using unmarked police cars, people expect such conduct, whereas tailing suspects for a month was impractical and therefore unexpected. If that was indeed Justice Alito's rationale, our survey data show that the rationale turns out not to be a good prediction of what the public actually expects. See Tables 1–3. Note also Table 5, which indicates that our respondents rarely think about expectations of privacy in ways tied to the state's expenditures on surveillance. In any event, our survey tests the congruence between expectations and the shadow holding in Justice Alito's opinion rather than testing sentiment regarding any particular rationale for that holding.

[31] 690 F3d 772 (6th Cir 2012).

est cell-phone towers amounted to a Fourth Amendment search.[32] The cell-tower information led them to the suspect's mobile home, where they discovered large quantities of marijuana and two semi-automatic weapons. The Sixth Circuit used at its starting point Justice Alito's opinion, and viewed the difference between twenty-eight-day tracking and three-day tracking as constitutionally dispositive:

> Justice Alito's concurrence and the majority in *Jones* both recognized that there is little precedent for what constitutes a level of comprehensive tracking that would violate the Fourth Amendment. Skinner's case, however, comes nowhere near that line. While *Jones* involved intensive monitoring over a 28-day period, here the DEA agents only tracked Skinner's cell phone for three days. Such "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." Id. at 964 (Alito, J., concurring).[33]

In a subsequent case, a federal district court in Michigan applied *Skinner* and deemed real-time surveillance of several cell phones that lasted between thirty and forty-five days to be a search, requiring a warrant supported by probable cause.[34] The boundary between permissible and impermissible warrantless real-time surveillance of geolocation in the Sixth Circuit is therefore somewhere between three and twenty-nine days.[35] Another decision, also from a district court in Michigan, went even further than the Court in *Jones* and held that a warrant allowing for cell-phone GPS tracking for a thirty-day period was invalid for lack of particularity.[36] According to that court, such prolonged surveillance was so troublesome that, absent minimization procedures, "[t]he tracking warrants were akin to the general warrants condemned by the Founders and are repugnant to the Fourth Amendment."[37]

---

[32] Id at 776.

[33] Id at 780 (internal citations omitted).

[34] *United States v Powell*, 943 F Supp 2d 759, 774 (ED Mich 2013). Although the *Powell* Court found that warrants backed by probable cause were required, id at 778, 780, it nevertheless deemed the geolocation admissible under the good-faith exception to the exclusionary rule. Id at 783–84.

[35] See also *Commonwealth v Augustine*, 4 NE3d 846, 865 (Mass 2014) (applying the Alito *Jones* framework to historical cell-site tracking information and deeming the collection of two weeks' worth of geolocation information without a warrant to violate the state constitution).

[36] See *United States v White*, 62 F Supp 3d 614, 627 (ED Mich 2014).

[37] Id at 617. Again, however, the suppression motion was denied under the good-faith exception. See note 34.

In *United States v Graham*, the Fourth Circuit treated the government's collection of even two weeks' worth of cell-site location information as a Fourth Amendment search.[38] Dissenting in *Graham*, Judge Diana Gribbon Motz accused her colleagues of trying "to beat the Supreme Court to the punch" of overruling its prior precedents applying *Katz* and the third-party doctrine.[39] Other courts have been similarly divided over the implications of Justice Alito's opinion. In *United States v Davis*, an en banc decision in the Eleventh Circuit, the majority argued that the Alito and Sotomayor concurrences altered nothing, the dissenter argued that the game has permanently changed, and three separate concurring opinions expressed different understandings of the governing law.[40]

The Florida Supreme Court's opinion in *Tracey v State*[41] provides yet another approach to *Jones*. The court in *Tracey* reviewed the various concurring opinions in *Jones* and concluded that the duration of monitoring could not be constitutionally decisive.[42] Distinguishing the Supreme Court's 1983 decision in *Knotts*, the court found that tracking Tracey's cell phone in real time on public roads for one day without a warrant violated the Fourth Amendment.[43] Surveillance duration was therefore irrelevant because such police action was a search regardless of its duration. Other courts have held that warrantless cell-phone tracking for just one evening constitutes a search under their state constitutions.[44]

---

[38] *United States v Graham*, 796 F3d 332 (4th Cir 2015). The Fourth Circuit has voted to reconsider its opinion in *Graham* en banc. See *United States v Graham*, 2015 WL 6531272 (Oct 28, 2015).

[39] Graham, 796 F3d at 390 (Motz dissenting).

[40] *United States v Davis*, 785 F3d 498 (11th Cir 2015) (en banc). Indeed, the district court considering *Jones* on remand opined that Justice Alito's proposed distinction between short-term surveillance and long-term surveillance was not the law. See *United States v Jones*, 908 F Supp 2d 203, 213–14 (DDC 2012). The district court held the evidence admissible under the good-faith exception to the exclusionary rule. Id at 214–16.

[41] 152 So3d 504 (Fla 2014).

[42] Id at 520 ("[B]asing the determination as to whether warrantless real time cell-site location tracking violates the Fourth Amendment on the length of the time the cell phone is monitored is not a workable analysis. It requires case-by-case, after-the-fact, ad hoc determinations whether the length of the monitoring crossed the threshold of the Fourth Amendment in each case challenged.").

[43] Id at 525–26.

[44] See, for example, *State v Earls*, 70 A3d 630, 644 (NJ 2013) ("[W]e hold today that police must obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information through the use of a cell phone. …

With these disparate approaches, we have seen the federal and state courts fragment every which way on the duration question foregrounded by Justice Alito's opinion in *Jones*. Some judges, like those in *Skinner*, apply the Alito framework and deem warrantless short-term geolocation surveillance constitutionally permissible and warrantless long-term surveillance impermissible.[45] Other judges, as in *Davis*, ignore the duration of geolocation surveillance, and hold both long- and short-term surveillance permissible.[46] Finally, still other judges, as in *Tracey*, reject the salience of surveillance duration by holding even very short-term warrantless geolocation tracking impermissible.[47] The Supreme Court will need to revisit the salience of duration in the constitutional analysis soon. In Part II, we argue that the Supreme Court should consider public opinion data when it does so.

## II. The Katz Framework's Ambiguity

Under *Katz*, whether police conduct constitutes a "search" depends on whether it violates a person's actual expectation of privacy and whether society is prepared to recognize that subjective expectation as reasonable. Getting the target of surveillance to describe his own privacy expectations honestly is quite challenging, and there is little normative reason to care what any particular defendant thought.[48] One response to these problems is to ask a large number of disinterested people whether they would have expected privacy were they in the target's shoes. These responses can then become a good proxy for what the target of surveillance should have actually expected and, more importantly, provide law enforcement with direct evidence of what expectations are commonly held. As it happens, however, there are disputes among both jurists and scholars as

Our ruling today is based solely on the State Constitution. We recognize that *Jones* and *Smith*, to the extent they apply, would not require a warrant in this case.").

[45] See notes 31–37 and accompanying text.

[46] *United States v Wilford*, 961 F Supp 2d 740, 772 (D Md 2013) ("But the mosaic theory was not adopted as a holding by the Supreme Court, nor has it been endorsed by the Fourth Circuit. And, it appears somewhat unworkable in practice."); see also *United States v Barraza-Maldonado*, 879 F Supp 2d 1022, 1029 (D Minn 2012) (ignoring the duration of surveillance under *Katz* and *Jones* in deeming the police's use of GPS tracking on a vehicle constitutionally permissible); *State v Drayton*, 411 SC 533 (SC App 2015) (following the subsequently reversed district court opinion in *Graham*, not *Tracey*).

[47] See *Earls*, 70 A3d at 630.

[48] See note 148.

to whether it is appropriate to consult survey data in determining the meaning of "expectations of privacy" and the related question of whether those expectations are "reasonable." The debate is presently unresolved and it continues to preoccupy at least some Justices on the Court. In this part we highlight some prominent recent judicial and scholarly statements about Fourth Amendment methodologies. We also present a normative case for integrating survey research into *Katz* doctrine, building on important work previously done by Christopher Slobogin.

### A. ARE ACTUAL BELIEFS ACTUALLY RELEVANT?

Justice Alito is the member of the Court who seems most interested in exploring the relevance of what ordinary people actually believe about searches. A recent exchange highlights his frustration with the present uncertainty over Fourth Amendment methodologies. In October Term 2013, the Court held that, absent exigent circumstances, it will usually be unreasonable for law enforcement to conduct a warrantless search of a suspect's cell phone incident to his arrest.[49] During the oral argument for what would become the Court's opinion in *Riley v California*, Justice Alito asked Judith Mizner, an Assistant Federal Public Defender, on at least four different occasions: "On what basis does the Supreme Court conclude that a reasonable expectation of privacy exists?"[50] The answer he was apparently sympathetic to, which Mizner never provided, appeared in Alito's *Jones* concurrence, where he equated Fourth Amendment reasonable expectations of privacy with "popular attitudes," and warned of the dangers that arise when judges gauge these attitudes by projecting their own beliefs onto those of the public as a whole.[51] In *Jones*, he referred at various times to reasonable expectations of pri-

---

[49] *Riley*, 134 S Ct at 3495.

[50] *United States v Wurie* (US April 29, 2014), Oral Argument Transcript, available at 2014 WL 1694920, at *39–*41. *Wurie* and *Riley* were consolidated into the *Riley* opinion. Justice Souter posed essentially the same question to Kenneth Lerner, the lawyer for Danny Kyllo in the landmark Fourth Amendment case of *Kyllo v United States*, 533 US 27 (2001). See Oral Argument Transcript in *Kyllo v United States*, 2001 WL 168056, at *19 (Feb 20, 2001) ("Justice Souter: So you're saying that reasonable expectation is in part based on fact, what you do, in fact, expect, and that informs, should inform the standard of reasonable expectation, is that the nub of what you're saying?" "Mr. Lerner: Yes. It is partly what we all expect.").

[51] Jones, 132 S Ct at 957, 962 (Alito, J, concurring) ("[J]udges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz*

vacy as "the average person's expectations about the privacy of his or her movements,"[52] treated "popular expectations" and "popular attitudes" as synonymous,[53] and referenced the "circularity" of *Katz*'s reasonable expectation of privacy test. Of course, circularity is only an intelligible concern if public attitudes are the guiding force in the *Katz* test.[54] He also differentiated between what the public may prefer and what it may nevertheless believe and expect.[55] Finally, he criticized Justice Scalia's majority opinion for embracing a vision of the Constitution that treats technological surveillance as a search, but old-fashioned surveillance that yields the same quantum of information as a nonsearch.[56]

To be sure, there is some ambiguity about what methodology Justice Alito was applying in his concurring opinion.[57] But, on the

---

test looks. In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce *significant changes in popular attitudes*.") (emphasis added).

[52] Id at 963.

[53] Id at 962 ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

[54] Id ("The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks.") (citations omitted). The circularity critique holds that popular attitudes dictate judicial pronouncements about the state of the law, which in turn dictate popular attitudes. See Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L Rev 1, 60–62 (2001); Jed Rubenfeld, *The End of Privacy*, 61 Stan L Rev 101, 106–07 (2009). During oral arguments for *City of Los Angeles v Patel*, Justice Kennedy asked counsel: "If you prevail in this case and a member of the Court sits down to write the opinion, does he or she have to use the phrase "reasonable expectation of privacy" and say there is no reasonable expectation of privacy in our society, in our culture, in our day, or do we just forget that phrase? In in a way, *as we all know it's circular, that if we say there is a reasonable expectation, then there is*." See *City of Los Angeles v Patel* (Mar 3, 2015), Oral Argument Transcript, available at 2015 WL 888287, at *13 (emphasis added).

[55] *Jones*, 132 S Ct at 957, 962 (Alito, J, concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

[56] Id at 961 ("Second, the Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.").

[57] Most puzzlingly, Justice Alito writes: "The Court argues—*and I agree*—that 'we must "assure preservation of that degree of privacy against government that existed when the

whole, his oral argument questioning in *Riley* and his concurring opinion in *Jones* elevated the importance of the average member of the public's actual beliefs and suggested their centrality to the *Katz* inquiry.

We agree with Justice Alito's apparent approach to this basic jurisprudential question and we show how scientific polling can alleviate concerns that, in undertaking such an inquiry, judges will place undue weight on their own beliefs or on the beliefs of people in their social orbits. We posit that under *Katz*, the Court should recognize subjective expectations of privacy under the Fourth Amendment when it finds as an empirical matter that contemporary, ordinary Americans expect privacy in a particular context.

### B. FOUR MODELS OF THE FOURTH AMENDMENT?

*Katz*'s two-prong test focuses both on whether the target of surveillance has a subjective expectation of privacy and whether that expectation is one that society is prepared to recognize as reasonable.[58] Confusion has abounded in the decades since *Katz* about precisely what Justice Harlan meant when he articulated the test and what the Court itself took it to mean. The consensus in the scholarship on *Katz*'s first prong seems to be something like this. *Katz* prong 1 is nearly always a nonissue because it is generally safe to assume a criminal defendant would not have exposed incriminating information unless she believed she was not being monitored. This view is nicely encapsulated in a recent article by Orin Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*.[59]

Most of the scholarly and judicial discussion of *Katz* has therefore focused on the second prong of the test: whether the privacy expectations are of a sort "that society is prepared to recognize as 'rea-

Fourth Amendment was adopted."' But it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." Id at 958 (emphasis added) (citation omitted). Justice Alito does not develop this thought any further, but there is little reason to expect continuity in attitudes between eighteenth-century Americans and twenty-first-century Americans.

[58] See note 26 and accompanying text.

[59] Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U Chi L Rev 113 (2015); see also Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L Rev 409, 429 (2007) ("[I]n striking an appropriate balance between the two prongs of the *Katz* test, the Court has chosen to weigh far more heavily the objective reasonableness inquiry.").

sonable.'" Kerr has done important work in this area as well. In his 2007 article, *Four Models of Fourth Amendment Protection*, he identifies four distinct threads in Supreme Court jurisprudence that reflect divergent understandings of *Katz*'s second prong.[60] The first is what Kerr calls the "probabilistic model." This is a purely descriptive approach, one that "tries to assess the likelihood that a person will be observed or a place investigated based on prevailing social practices."[61] Kerr's second approach is the "the private facts model." This model focuses on the sensitivity of the information at issue—if "the government obtains information that is particularly private, then the acquisition of that information is a search."[62] A third possibility is the "positive law model." Under this approach, the courts are to determine whether the government's conduct would run afoul of some independent legal framework.[63] If the police enter the interior of a home, for example, that is a search because it is also a trespass. Kerr notes that, in addition to property law, federal regulations may also affect reasonable expectations of privacy under this model.[64] Finally, Kerr identifies the "policy model" under which the existence of a search depends on the answer to a utilitarian balancing inquiry. Under this approach, "[j]udges must consider the consequences of regulating a particular type of government activity, weigh privacy and security interests, and opt for the better rule."[65]

Kerr provides a long list of examples in which the Supreme Court has embraced, rejected, or ignored these four approaches to addressing *Katz*'s second prong.[66] Sometimes several models are applied to the same case by the Court, and sometimes the Court implausibly claims its cases are methodologically consistent. Kerr argues that this state of affairs, in which the Court decides in each case which of

---

[60] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan L Rev 503 (2007). Kerr's article has already been cited by seven different courts, as of December 2014.

[61] Id at 508.

[62] Id at 512.

[63] Id at 516–18.

[64] Id at 517 (citing *Florida v Riley*, 488 US 445 (1989)).

[65] Id at 519.

[66] Id at 509–22. Kerr observes that the Court has never criticized the policy model, but they have ignored it plenty of times. Id at 521–22. Compare Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 Utah L Rev 977, 1022–23 (identifying the Supreme Court's inconsistent approaches to determining the reasonableness of searches over time).

these four models to apply, is desirable.[67] We disagree, because this approach creates an undue risk of doctrinal incoherence and unpredictability.[68]

It is worth emphasizing that Kerr's helpful framework for analyzing Fourth Amendment expectations predates *Jones*. *Jones* itself removes the "positive law" model from the *Katz* framework, instead requiring that courts decide *before reaching the Katz questions* whether law enforcement conduct violated independent rights under applicable state property law.[69] After *Jones*, we might then regard the pre-*Katz* trespass/positive law inquiry as the precursor to *Katz*'s application. Justice Alito's opinion, on the other hand, argues in favor of integrating the question of what the positive law says into the *Katz* framework itself.[70] Finally, while Kerr is right that the Supreme Court often considers cost-benefit analysis germane to *Katz* prong 2 under the policy model, we believe the correct place to incorporate such analysis is the reasonableness inquiry that courts turn to if they decide that particular police conduct constitutes a Fourth Amendment search.[71] That reasonableness inquiry determines whether a warrant or something less is required before the search can commence.

The *Katz* framework has become incoherent and inconsistent, but it need not remain so. Under our approach, the positive law model would be applied to determine whether courts even need to reach

---

[67] Kerr, 60 Stan L Rev at 542 (cited in note 60).

[68] It has also been argued that all of these models collapse into an overall assessment of intrusiveness. See, for example, Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 Minn L Rev 1588, 1603 (2010).

[69] *Jones*, 132 S Ct at 950–51. The same methodology was employed by a majority of the Court in the subsequent Fourth Amendment search case of *Florida v Jardines*, 133 S Ct 1409, 1417 (2013). The Court said that because the police's use of a drug-sniffing dog on Jardines's porch would have been a trespass and thus a search, it was unnecessary for the courts to consider the *Katz* framework. Id.

[70] *Jones*, 132 S Ct at 959–60 (Alito, J, concurring).

[71] For descriptions of the Supreme Court's turn toward cost-benefit balancing in Fourth Amendment reasonableness doctrine, see Slobogin, *Privacy at Risk* at 21–47 (cited in note 24) (developing a proportionality principle of the Fourth Amendment and showing how it is consistent with some of the Supreme Court's case law); Clancy, 2004 Utah L Rev at 1003–15 (cited in note 66) (discussing the courts' use of the balancing approach to Fourth Amendment reasonableness determinations); Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L Rev 199, 223–47 (1993) (discussing the evolution of the case law during the Warren Court era); Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 Miss L J 1133, 1159–60 (2012) (advocating a balancing approach that is not deferential to government actors' asserted interests).

the *Katz* question, and the probabilistic model would become the *Katz* prong 1 inquiry—it asks whether people in general expect privacy in a given situation and uses this as a proxy for what the target of surveillance expected. Courts deciding whether society is prepared to recognize a subjective expectation of privacy as reasonable (*Katz* prong 2) would then apply the private-facts model; if the privacy expectation only serves to hide unlawful conduct and cannot reveal any other sensitive information, then it would not be a search. And, finally, if surveillance was deemed to be a search, courts would apply the policy model to determine whether it was reasonable for the state to conduct that search without a warrant. All four of the factors Kerr identified in the case law would remain relevant, but each would now have one doctrinal hook. This approach is clearer than the status quo, where courts selectively ignore factors or try to cram multiple factors into *Katz* prong 2 without explaining how they interact. In instances where the results of a judicial cost-benefit analysis were clear but the result of the *Katz* test was murky, the courts could continue to assume that there was a subjective expectation of privacy that society is prepared to recognize but find no Fourth Amendment violation on the basis of the reasonableness of the warrantless search. The Supreme Court did precisely that in the *Quon* case.[72]

Under our approach, *Katz* prong 1 would become more significant and *Katz* prong 2 would become less contentious and less frequently fatal to targets of surveillance. Compared to the muddled status quo, courts collectively would likely find there to be more searches. Put another way, prong 1 would be satisfied in many cases that are currently doctrinally marginal and prong 2 would treat more surveillance as searches than it presently does. But this shift would not drastically expand the warrant requirement. The constitution forbids only unreasonable searches, and judges would consider the benefits of surveillance in the post-*Katz* reasonableness inquiry. This would likely lead courts to bless an increased number of warrantless searches. This doctrinal reshuffle would have two major practical effects. First, judges would be forced to be explicit when they wish to override privacy expectations in the name of law enforcement efficiency. This would likely lead to more carefully considered and more limited divergences from actual privacy expectations. Second,

[72] *City of Ontario, California v Quon*, 560 US 746, 760–65 (2010).

there may be some cases in which the American people do not expect privacy but judges think they ought to. Under our approach, judges would not be able to override privacy expectations in that direction. As our data indicate, however, those instances in which the American public by and large does not expect privacy are ones in which current doctrine would almost certainly not provide protection. For example, Americans generally expect that if they are in a public park the police can use silent video surveillance to watch them.[73] This expectation lines up quite well with judicial interpretations of the Fourth Amendment.[74] Though we do not have enough data to know for sure, it may be that there are no cases in which current doctrine *would* protect privacy and the public's actual expectations would *not*.[75]

### C. SURVEYS AS A MORE SATISFYING METHODOLOGY

Ordinary people's views sometimes help shape the Court's views of the Constitution's meaning. To offer a couple of high-profile examples, changing popular views about same-sex marriage mattered in *Obergefell*,[76] and shifting beliefs about the death penalty for juveniles, reflected in state-level legal changes, mattered in *Roper v Simmons*.[77] Indeed, although there are occasional instances in which the Court acts in a countermajoritarian fashion, the Supreme Court generally interprets the Constitution in a manner that is consistent with public opinion.[78] Against that backdrop, we think the case for

---

[73] See Table 9.

[74] See note 199.

[75] There may, however, be situations that would be searches under current doctrine but fail under our understanding of prong 2.

[76] *Obergefell v Hodges*, 135 S Ct 2584, 2603 (2015) ("[I]n interpreting the Equal Protection Clause, the Court has recognized that new insights and societal understandings can reveal unjustified inequality within our most fundamental institutions that once passed unnoticed and unchallenged.").

[77] 543 US 551, 564–68 (2005) (striking down the juvenile death penalty under the Eighth Amendment's "evolving standards of decency" test in light of shifting state practices).

[78] Robert G McCloskey, *The American Supreme Court* 260 (Chicago, 5th ed 2010) (revised by Sanford Levinson) ("One of the main points to emerge from this study is that the interests and values, and hence the role, of the Court have shifted fundamentally and often in the presence of shifting national conditions. . . . Indeed, the facts of the Court's history impellingly suggest a flexible and nondogmatic institution fully alive to such realities as the drift of public opinion and the distribution of power in the American republic. . . . [I]t is hard to find a single historical instance when the Court has stood firm for very long against a really clear wave of public demand."); Barry Friedman, *The Will of the People: How Public Opinion Has*

incorporating stable popular expectations into Fourth Amendment analysis is relatively strong. First, the Court has been doing this for decades in the context of figuring out what constitutes a search. Probabilistic model cases like *Bond v United States*,[79] *Minnesota v Olson*,[80] and *California v Carney*,[81] among many others,[82] make that plain enough. Writing on a blank slate, it would be sensible to argue that popular attitudes should influence surveillance law only to the extent that those attitudes affect the content of legislation. But adopting that view now, after the Court has repeatedly indicated that constitutional law will play a major role in regulating run-of-the-mill surveillance, after Congress had shown that it intends to defer often to the courts in this area, and after many Fourth Amendment decisions have elevated the salience of popular expectations, is less appealing. Second, the Fourth Amendment is designed to sort between surveillance that is costly enough to justify the imposition of a warrant requirement and surveillance whose privacy costs are less significant. It is theoretically possible to sort between serious and nonserious privacy harms without looking at what ordinary people want and expect. But, for reasons we discuss below, ignoring popular attitudes is less appealing than taking them into account.

That said, in our view, the role for survey data in Fourth Amendment analysis is important but limited. It is appropriate to ask laypeople whether they expect particular police conduct, how much it bothers them, and whether such conduct might reveal sensitive or embarrassing information. People can give meaningful and reasonably well-informed responses to these questions, and these are the kinds of data we will present in Part III. We think asking peo-

*Influenced the Supreme Court and Shaped the Meaning of the Constitution* 13–14 (Farrar, Straus and Giroux, 2009) ("[O]ver time, as Americans have the opportunity to think through constitutional issues, Supreme Court decisions tend to converge with the considered judgment of the American people. . . . On issue after contentious issue—abortion, affirmative action, gay rights, and the death penalty, to name a few—the Supreme Court has rendered decisions that meet with popular approval and find support in the latest Gallup Poll."). Gerry Rosenberg has articulated skepticism about claims that the Supreme Court's interpretations of the Constitution influence popular beliefs, a skepticism we share. See Gerald N. Rosenberg, Book Review, *The Wonder of It All*, 45 Tulsa L Rev 679, 686–87 (2009). Our hypothesis is that public views influence the Justices' views but that the Court's interpretations of the Constitution do little to influence public beliefs. See note 92.

[79] 529 US 334, 338–39 (2000).

[80] 495 US 91, 98–100 (1990).

[81] 471 US 386, 390–93 (1985).

[82] Kerr, 60 Stan L Rev at 508–10 (cited in note 60).

ple whether the benefits of police surveillance outweigh the costs is much less valuable. Most members of the public lack the expertise and information necessary to make those policy judgments.[83] Hence our doctrinal approach leaves those policy decisions in the hands of judges, who would continue to make post-*Katz* judgments about the reasonableness of a search, and legislatures, which could provide for greater privacy protections than the Fourth Amendment presently requires. We do think judges will do a better job of confronting these trade-offs when they have reliable information about the extent to which the public would be surprised and bothered by particular police tactics. The alternative is for judges to rely on their own intuitions and those of their clerks, which are unlikely to be representative.

In the remainder of this part we argue that public opinion data drawn from nationally representative samples of the population ought to be dispositive on the question of *Katz* prong 1. In our formulation, the question of whether there was a subjective expectation of privacy would be framed as whether people *in general* expect privacy in a given situation. Just as the *Jones* majority pulled the "positive law" question out of the *Katz* framework, we would pull the "probabilistic" inquiry out of prong 2, and make it the central question under *Katz* prong 1. A defendant wishing to claim that a surveillance strategy constitutes a search would need to show that the populace[84] generally regards the law enforcement conduct in question as a violation of privacy expectations. With positive law already consigned to a pre-*Katz* inquiry by *Jones*,[85] our approach would permit courts to distill *Katz* prong 2 down to the "private-facts" inquiry. This would allow for more objective results than the cost-benefit balancing inquiry (i.e., Kerr's "policy model") and, unlike the policy model, it isn't duplicated elsewhere in Fourth Amendment law.[86]

---

[83] Some other empirical research asks respondents to make these normative judgments. See note 113.

[84] See note 149 for elaboration on how the populace might be defined.

[85] After Justice Scalia's death there are only four remaining votes on the Supreme Court favoring the disaggregation of the positive law framework from the *Katz* approach. The law in this area may well hinge on the views of Justice Scalia's eventual replacement.

[86] See text accompanying notes 157–63.

We feel that focusing *Katz* prong 1 on an empirical question is normatively desirable.[87] The Fourth Amendment is designed to safeguard individuals against governmental overreach. When there is a sharp divide between what the courts describe as the Fourth Amendment's scope and what the people actually expect the Fourth Amendment's scope to be, various problems arise. Law-abiding people may take excessive precautions to protect their information, keeping it not only from the state's agents but also from third parties who could put the information to productive uses.[88] Or citizens might make inordinate investments in learning the contours of Fourth Amendment law, time and money that could be better spent elsewhere. Also, mistaken expectations limit the effectiveness of the democratic process as a check on law enforcement surveillance; the public may not move legislatively to protect privacy if they mistakenly believe it is already protected constitutionally. Disconnects between actual law and perceived law may also provide police officers and prosecutors with undue leverage over citizens. Although figuring out whether various possible interpretations of the Fourth Amendment enhance social welfare is a tricky business, we think there is a strong case to be made that misalignment between the law and social expectations is detrimental for both efficiency and fairness-related reasons. So even though an empirical vision of "reasonable expectations of privacy" isn't what Justice Harlan had in mind when he penned his *Katz* concurrence,[89] there are good reasons why ordinary citizens' actual beliefs have become more doctrinally salient in the years that followed.[90]

---

[87] See also text accompanying notes 123–25 for further development of our normative argument. For different, but largely congenial, accounts that argue for the centrality of privacy expectations in Fourth Amendment inquiries, see Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 Tex Tech L Rev 143, 157–62 (2015); Slobogin, 94 Minn L Rev at 1602–04, 08 (cited in note 68).

[88] See Thomas P. Crocker, *The Political Fourth Amendment*, 88 Wash U L Rev 303, 368–78 (2010); William J. Stuntz, *Waiving Rights in Criminal Procedure*, 75 Va L Rev 761, 794 (1989); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 Hastings L J 645, 720 (1985).

[89] See text accompanying note 26; Kerr, 82 U Chi L Rev at 124 (cited in note 59).

[90] To be clear, while there are Fourth Amendment decisions like *Kyllo* and *Jardines* in which originalist considerations of what Founding Era citizens would have expected play a role, we do not regard the basic *Katz* test as remotely originalist. See generally *Kyllo v United States*, 533 US 27 (2001); *Florida v Jardines*, 133 S Ct 1409 (2013). Nor do we think that present jurists interpreting *Katz* owe a duty of fidelity to whatever Justice Harlan intended when he penned his concurrence in that case. Popular expectations of privacy do change over

*Katz* prong 1 is, of course, only part of the threshold Fourth Amendment calculus. Though we think that it should become the focal point for data-driven Fourth Amendment decision making, there are other places where incorporating survey results from nationally representative samples could improve judicial decision making. Namely, prong 2 of *Katz* asks whether society is prepared to recognize a subjective expectation of privacy as reasonable, and data about the degree to which Americans regard particular information as sensitive and embarrassing (Kerr's "private-facts" model) could figure in to this calculus.

It is important at this stage to underscore the difference between two related but distinct empirical questions. One involves the privacy *expectations* of ordinary Americans. The other examines the degree of perceived intrusion, embarrassment, and personal exposure created by the surveillance. These two inquiries are conceptually independent.[91] An example may help. A frequent flier will likely *expect* deeply intrusive searches at airport security, but may still be embarrassed by them and concerned that they will reveal sensitive personal information. Thus expectations are not violated, but intrusion still occurs. Conversely, a person might be greatly surprised if the government scrutinized his monthly natural gas utility bills for the last several years, but may not feel the search embarrassed him or revealed anything of importance about him. In our formulation, the perceived intrusiveness of a search is relevant under *Katz* prong 2, but the expectations of ordinary Americans should be dispositive under *Katz* prong 1.

How would researchers go about measuring the public's expectations of privacy? The most obvious approach would be the one we use here, which is to ask a representative sample of Americans such questions directly. There will inevitably be some heterogeneity

time, and under the *Katz* line of cases it is implicit that the scope of constitutional protections will similarly fluctuate. See Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 BC L Rev 1, 71 (2013). Even originalism-friendly opinions like *Jardines* devote more space to discussing contemporary norms than Founding Era norms, in part because evidence of the latter is so difficult to come by. *Jardines*, 133 S Ct at 1414–16. For a persuasive critique of Fourth Amendment originalism, see David A. Sklansky, *The Fourth Amendment and Common Law*, 100 Colum L Rev 1739 (2000). The question of how much privacy expectations change over time is part of a long-term project that we are just beginning. See note 146.

[91] As a practical matter, there are some connections between expectations and intrusiveness. See text accompanying note 158.

in responses, but we should expect to find broad consensus around many questions involving law enforcement surveillance.[92] There are at least two possible weaknesses to this approach. The first is that there may be a disconnect between actual and reported attitudes. Survey instruments rely on cheap talk by respondents. Respondents have no real skin in the game when we are asking them about their privacy expectations, and researchers employ no lie detectors. As a result, respondents might answer questions in a way that reflects their aspirations rather than their true expectations.[93]

The problem of insincere respondents can never be discounted completely, but it is one with which psychology and the other social sciences have come to terms. That isn't to say that data about the revealed preferences of Americans when it comes to privacy wouldn't be better. They may be,[94] but they are very difficult to collect,[95] especially in the same quantities that we are able to report here. Comfortingly, the available evidence from various well-designed surveys is broadly consistent with observational studies of revealed preferences.[96] In fact, there is a large empirical liter-

---

[92] See generally Christopher Slobogin and 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); Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 82 U Chi L Rev 1165 (2014). In subsequent work, we will draw on other data we have collected to show that it is common for there to be lay consensus on Fourth Amendment questions. See Matthew B. Kugler and Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity* (in progress).

[93] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 BC L Rev 1511, 1522–23 (2010).

[94] One approach to collecting such data in the privacy domain is described in Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U Chi L Rev 919, 934–39, 970–73, 983–85 (2005) (discussing whether for the purposes of invasion of privacy tort claims, "reasonable expectations of privacy" should be based on survey research results or observational studies of consumer behavior that utilize social network theory).

[95] The price system sometimes permits the analysis of revealed preferences through large data sets. Unfortunately, the price system does rather little to reveal the private value that Americans place on keeping the government from learning information about them. For example, when someone decides to build a fence around her home, it is difficult to determine the extent to which the purchase was driven by privacy concerns and the extent to which it was driven by security concerns (thwarting trespassers, deterring burglars, etc.). Disentangling the two likely requires surveying the purchaser, which brings us back to square one. The same entanglement can occur online, with nearly all privacy enhancements acting as simultaneous security enhancements.

[96] See Sampo V. Paunonen, *Big Five Factors of Personality and Replicated Predictions of Behavior*, 84 J Personality & Soc Psych 411, 413–21 (2003) (surveying the literature and reporting on the results of original experiments designed to test correlations between survey responses and observed behavior).

ature showing that sufficiently specific attitude measures are often very good predictors of behavior.[97] Social scientists also can use survey strategies to weed out disinterested or insincere respondents, thereby enhancing the correlation between survey responses and actual beliefs. We describe our use of this technique below.[98]

The second potential weakness is that consultation of public attitudes may lead to circularity. By this account, social expectations will change as the law does, so that expectations will eventually conform to policies that were initially rejected.[99] There are two variations on the circularity claim. The first is a story about information dissemination and public opinion updating. On this account, when courts make a good-faith interpretation of the law, members of the public hear about it and update their prior beliefs. To lay our cards on the table, we are unimpressed with this claim. As part of a future project, we have collected significant amounts of data about the extent to which well-publicized legal changes affect ordinary Americans' articulated expectations of privacy. Those data, which will form the core of our next paper, indicate that even prominent Fourth Amendment decisions respondents say they have heard about move the needle of Americans' articulated expectations of privacy very little.[100] A unanimous, well-publicized *Supreme Court* opinion on cellphone privacy barely affected public expectations on the issue before the Court, and this was true whether respondents were questioned a week after the decision was handed down or nearly a year later. Based on the data we have collected, we would be surprised if any Fourth Amendment decision other than *Miranda*[101] has permeated popular culture and discourse enough to alter significantly the public's expectations about what the police can do.

---

[97] See Icek Ajzen and Martin Fishbein, *Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research*, 84 Psych Bull 888 (1977); Jens Hainmueller, Dominik Hangartner, and Teppei Yamamoto, *Validating Vignette and Conjoint Survey Experiments Against Real-World Behavior*, 112 Proceedings of the National Academy of Sciences 2395 (2015); Jason T. Siegel et al, *Attitude-Behavior Consistency, the Principle of Compatibility, and Organ Donation: A Classic Innovation*, 33 Health Psych 1084 (2014).

[98] See text accompanying note 164.

[99] *Jones*, 132 S Ct at 962 (Alito, J, concurring) ("The *Katz* reasonable expectation of privacy test . . . involves a degree of circularity.").

[100] See Kugler and Strahilevitz, *The Myth of Fourth Amendment Circularity* (in progress) (cited in note 92).

[101] *Miranda v Arizona*, 384 US 436 (1966).

A more sinister circularity story suggests that expectations of privacy can be conditioned. If the President announces on national television that all private residences are now subject to warrantless searches, then people will come to expect such searches.[102] The conditioned-expectations story posits that government actors will proceed in bad faith to expand their power at the expense of the citizenry. Not surprisingly, when the conditioned-response argument is made in the modern American context it is always articulated as a hypothetical. No court or credible scholar has pointed to an instance of a power-hungry elected official acting in such a manner and getting away with it. The conditioned-response story assumes away the inevitable popular counterreaction to transparent government overreaching. Individuals can no doubt be conditioned, but conditioning a hostile body politic in a democratic regime is extremely difficult.[103] And government officials in democracies understand that announcing broad, new, invasive searches that are deeply unpopular is foolhardy, which is why conditioning narratives remain hypothetical. In sum, proponents of the circularity hypothesis overestimate both the visibility and moral authority of government pronouncements with the public. Our data indicate that the real-world effects of the Fourth Amendment's supposed circularity problem are overblown.

Other scholars have previously advocated assessing "reasonable expectations of privacy" using a survey instrument. Christopher Slobogin is the legal scholar who has pioneered this approach.[104]

---

[102] *Smith v Maryland*, 442 US 735, 741 n 5 (1979); Kerr, 60 Stan L Rev at 532 (cited in note 60) ("[I]magine the government announced that the FBI is tapping every single telephone call in the United States to listen for evidence of criminal activity. The invasions of privacy would be extraordinarily severe but no reasonable person would expect privacy in their calls after learning of this fact.").

[103] Arguably Facebook has succeeded in conditioning its users over a lengthy period of time to have diminished expectations of privacy. Paul Ohm, *Branding Privacy*, 97 Minn L Rev 907, 919–22 (2013). Yet even Facebook, which benefits from strong network effects, is obviously constrained by its users' existing preferences. When it takes steps that flout its users' privacy expectation and receives a negative reaction it typically apologizes and backtracks. See Ira S. Rubinstein and Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 Berkeley Tech L J 1333, 1392–1405 (2013).

[104] See, for example, Slobogin, *Privacy at Risk* (cited in note 24); Slobogin, 94 Minn L Rev at 1588 (cited in note 68); Slobogin and Schumacher, 42 Duke L J at 727 (cited in note 92).

Slobogin has surveyed students[105] and jury pool respondents[106] to gauge the perceived intrusiveness of various governmental surveillance techniques. A key finding from Slobogin's research is that while respondents' opinions typically track judicial attitudes about whether the technique at issue constitutes a "search" under the Fourth Amendment, scattered and important divergences do arise.[107] For example, under *Hoffa v United States*,[108] it is not a search for police to use undercover informants in criminal investigations, but respondents regard such government investigative techniques as more intrusive than other techniques that the courts have consistently held to be Fourth Amendment searches.[109]

An admitted problem with research by Slobogin and others is that it has not been conducted on a nationally representative sample of Americans.[110] Students obviously skew much younger than the general population, and the jury pool in a particular town will not reflect national sentiment. It is only in the last few years that legal scholars influenced by Slobogin's methods have begun examining the privacy preferences of Americans in a more empirically sound way. The trend owes much to the steeply declining costs of survey research. For example, in 2012 scholars at Berkeley commissioned a poll to assess the attitudes of Americans on the question of whether law enforcement should be required to get a warrant before searching a cell phone incident to an arrest.[111] Some of the same scholars followed up in 2014 with a nationally representative study of con-

---

[105] Slobogin and Schumacher, 42 Duke L J at 737 (cited in note 92). The identities of Slobogin's research subjects has troubled some, though the replication of several significant findings by other scholars using similar samples at different universities has alleviated a few concerns about the external validity of Slobogin's results. See Jeremy A. Blumenthal, Meera Adya, and Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing "Lay Expectations of Privacy,"* 11 U Pa J Const L 331, 344–45 (2009).

[106] Slobogin, *Privacy at Risk* at 111 (cited in note 24).

[107] Slobogin and Schumacher, 42 Duke L J at 739–42 (cited in note 92).

[108] 385 US 293 (1966); see also *United States v White*, 401 US 745, 752 (1971) (reaffirming *Hoffa*).

[109] Slobogin and Schumacher, 42 Duke L J at 740, 738 tbl 1 (cited in note 92) (noting that the use of a secretary as an undercover agent is deemed noticeably more intrusive by respondents than the search of an office drawer).

[110] See Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 Mich L Rev 951, 964 (2009).

[111] Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privacy* 10 (UC Berkeley Public Law Research Paper No 2103405, July 2012), archived at http://ssrn.com/abstract=2103405.

sumer privacy attitudes.[112] That said, no externally valid recent study delves deeply into Americans' Fourth Amendment attitudes.[113] While Slobogin himself has written about *Jones*, his paper on the subject did not draw on any new empirical research about public attitudes toward the mosaic theory, so he never posed Justice Alito's "duration sensitivity" question to research subjects.[114] As a result, there is a dearth of literature on what Americans actually believe with respect to the constitutional issues that the state and federal courts must decide every day. If a judge wanted to follow the probabilistic model in a given case, she would have to decide between relying on dated studies whose external validity has not been established[115] and

---

[112] Chris Jay Hoofnagle and Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L Rev 261 (2014).

[113] We know of only one additional contemporary paper that uses a nationally representative sample to track changes in attitudes about legal questions pending in the courts. See Katerina Linos and Kimberly Twist, *The Supreme Court, the Media, and Public Opinion: Comparing Experimental and Observational Methods* (2015 unpublished working paper, on file with authors). Linos and Twist's sophisticated paper does not examine any Fourth Amendment issues.

Another paper, which postdates ours by a little while, analyzes the public's normative attitudes about Fourth Amendment issues. See Christine S. Scott-Hayward, Henry F. Fradella, and Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age* (July 20, 2015 unpublished working paper, on file with authors). Though the Scott-Hayward and coauthors' paper is well done in many respects, our research strongly suggests that it suffers from external validity problems. Because of budgetary limitations, the paper uses a Mechanical Turk sample as a proxy for ordinary Americans' attitudes. Id at *41–*42. As our research shows, Mechanical Turk respondents are significantly more privacy-protective than the general U.S. population, perhaps because they skew younger. See note 171 and accompanying text. The size of the discrepancy between our representative sample and Mechanical Turk findings was large. We therefore believe that one should not use Mechanical Turk samples to assess the base-rate support for privacy-related beliefs in the general population. It may, however, still be valid to use such samples to evaluate the *relative* intrusiveness of searches. We do not have data specifically on that point. The Scott-Hayward paper also argues that the public's normative beliefs, not its expectations, are relevant, relying on the circularity hypothesis that our subsequent work debunks. Id at *39–*40.

We also note Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U Cin L Rev 207 (2013), and Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 SIU L J 475 (2012). Both studies have serious methodological problems relating to a lack of clarity about the sample composition, the unusual way results are reported, and the way questions were phrased.

[114] Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 Duke J Const L & Pub Pol 1 (2012). Slobogin's paper is more doctrinal than empirical, and it winds up proposing that surveillance lasting longer than 48 hours generally requires a warrant based on probable cause. Id at 24. The 48-hour threshold is not driven by his survey results. Our data show that this 48-hour distinction is not salient to American citizens. See Table 3 (showing very little difference in attitudes concerning one-day surveillance and one-week surveillance).

[115] Slobogin and Schumacher discuss the external validity of their research at Slobogin and Schumacher, 42 Duke L J at 745–51 (cited in note 92).

relying on guesswork, a straw poll of acquaintances, or other pseudo-scientific approaches.

Even setting aside questions about external validity, Slobogin's survey-based approach has been challenged on other grounds. Scholars wonder whether courts have the capacity to assess popular attitudes,[116] whether popular attitudes will fluctuate wildly from day to day,[117] why the content of constitutional provisions should hinge on those attitudes as opposed to doctrines grounded in prior constitutional and property-related precedents,[118] and whether popular attitudes about complicated legal and technological issues are meaningful.[119] Slobogin has responded to some of these criticisms, noting, for example, that courts routinely interpret survey results in other contexts, like trademark litigation.[120] And he points out that replication should alleviate concerns about random sample fluctuations.[121] We believe Slobogin acquits himself well in the debate, and our studies support many of his points. Notably, our own data on privacy expectations show nearly perfect stability over a time span of almost a year.[122]

That said, concerns about turning public opinion into constitutional doctrine remain. Absent the development of a public choice account for police practices and democratic failures, it is unclear why the content of constitutional law should depend on upholding popular sentiment. We have developed only a brief account here.[123] We do think that the case for placing real weight on survey responses is

[116] Kerr, 107 Mich L Rev at 965 (cited in note 110) ("How would judges know when public opinion has changed? And how should courts reconcile dueling surveys?").

[117] Id at 964 ("Results of a survey taken one day, with one audience, with questions phrased in a particular way may not match results from another day, another audience, and another set of questions.").

[118] See, for example, Solove, 51 BC L Rev at 1522 (cited in note 93); Daniel B. Yeager, *Search, Seizure, and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J Crim Law & Criminol 249 (1993).

[119] Solove, 51 BC L Rev at 1523 (cited in note 93).

[120] Slobogin, 94 Minn L Rev 1599–1600 (cited in note 68).

[121] Id at 1599.

[122] See Table 7A and Table 7B (comparing the results of Wave 3 to those of Waves 1 and 2); see also note 167 (noting that Wave 1 and Wave 2 of our surveys were statistically indistinguishable on questions concerning *Jones*).

[123] See text accompanying notes 87–90.

strongest when laypeople are being surveyed on issues that are familiar to them. For that reason, our surveys ask people about the sorts of technologies that they are likely to have encountered in the world, like email accounts, smartphones, car-based navigation systems, and computer webcams. With respect to less familiar technology, survey designers must do more work explaining the underlying technology to respondents, increasing the danger that responses will be influenced by the researchers' subjective judgments about how to describe the technology.

In assessing our approach it is important to avoid the mistake of comparing an admittedly imperfect survey-based methodology to an idealized alternative. If all judges were well-informed philosopher kings, then there would be good reasons to allow them to decide all Fourth Amendment questions on purely normative grounds. But judges are imperfect too. They have their own biases, their own limitations, and their own misimpressions,[124] and there is a danger that the effects of these biases will be magnified when constitutional law is decided by just nine people, three people, or one person. The system loses the benefits of aggregating the factual impressions of a large sample,[125] and enhances the risk that the idiosyncratic characteristics of the unrepresentative decision makers will systematically distort their assessments of the social tradeoffs. While we do not believe that laypeoples' naive priors are particularly useful to help courts resolve every constitutional question, we do think that they are informative in this context, particularly since the judges who are deciding Fourth Amendment cases are less likely than the broader populace to have been targeted or feel threatened by the surveillance techniques at issue. These naive priors will be informative, not decisive, precisely because *Katz* has more than one real prong under our approach.

Nevertheless, there are alternatives to basing "reasonable expectations of privacy" on what ordinary Americans actually say they

---

[124] See, for example, Lee Epstein, William M. Landes, and Richard A. Posner, *The Behavior of Federal Judges: A Theoretical and Empirical Study of Rational Choice* (Harvard, 2013).

[125] See, for example, Dhammika Dharmapala and Richard H. McAdams, *The Condorcet Jury Theorem and the Expressive Function of Law: A Theory of Informative Law*, 5 Am L & Econ Rev 1, 6–8 (2003); see also Cass R. Sunstein, *If People Would Be Outraged by Their Rulings, Should Judges Care?*, 60 Stan L Rev 155, 183–92 (2007) (describing the implications of the Condorcet jury theorem to judicial decision making).

expect. To recall Kerr's framework, the law might use precedents derived from external sources of law, like state property law, to define reasonable expectations.[126] Alternatively, the law might focus on how sensitive the information sought by the government is. Finally, the courts could engage in a utilitarian balancing calculus, weighing the privacy costs and security benefits of requiring a warrant when the government seeks information of a particular kind.[127] As we note above, there is a role for each of these frameworks to play in Fourth Amendment law, but incorporating survey data about public expectations and the costs of surveillance will make each of these inquiries less dependent on the life experiences and ideological priors of judges who happen to be resolving a case.

Consider a controversial problem in contemporary law—does the Fourth Amendment prohibit the National Security Agency's (NSA) warrantless collection of metadata concerning email and telephone traffic from tens of millions of Americans?[128] Figuring out whether the NSA's program satisfies a cost-benefit calculus is close to impossible given the limits of available knowledge.[129] Public opinion, however, furnishes one relevant data point in such a calculus by providing a measure of the extent to which the program enhances or diminishes Americans' sense of freedom and safety. These sorts of data can be obtained at a relatively low cost through the surveys

[126] For a thoughtful and extensive argument along these lines, see William Baude and James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv L Rev (forthcoming 2016) (unpublished draft on file with authors).

[127] See text accompanying notes 60–65. Of course, the courts could substitute a deontological framework for a consequentialist one in assessing the propriety of government surveillance. See Sklansky, 102 Cal L Rev at 1110–15 (cited in note 17).

[128] See generally *Klayman v Obama*, 957 F Supp 2d 1 (DDC 2013) (holding that parts of the NSA program are searches); *Smith v Obama*, 24 F Supp 3d 1005 (D Idaho 2014) (argued before 9th Circuit on appeal, Dec 8, 2014).

[129] Assuming the program is challenged in court within a few years of its implementation, nobody is likely to have a handle on the extent to which the program produces actionable intelligence, the costs of security officials' time spent responding to false leads generated by the program, the extent to which its existence chills commerce, the effect the program may have on political expression and the consequences for democracy of marginally more inhibited communications, the danger that information stored in the database will eventually fall into the hands of America's enemies through espionage or hacking, and a host of other pertinent considerations. Courts do their best to muddle through these extremely difficult issues, but it appears likely that at the time of the suit they will have before them reasonably accurate information about the government's out-of-pocket expenditures on the NSA program, some statements from civil libertarians expressing alarm at the existence of the program, and little else of probative value.

we describe below.[130] It is a sensible place to start the analysis even if it does not provide all the necessary answers.

A final point about the policy model is worth repeating. There is already plenty of room elsewhere in Fourth Amendment doctrine for the courts to engage in a cost-benefit balancing process. The determination that police conduct amounted to a search does not resolve the Fourth Amendment questions. Rather, once police conduct is found to have amounted to a search, the courts then shift their attention to the question of whether the police's conduct was reasonable.[131] As it has evolved in recent decades, this judicial inquiry often focuses on a balancing approach that weighs the costs and benefits of the government conduct at issue.[132] Considering the utilitarian calculus with respect to both the scope of the Fourth Amendment *and also* the level of process that reasonableness requires has the effect of double counting utilitarian interests, potentially slanting the doctrine against finding violations of the Constitution.[133] We regard that essential part of Fourth Amendment analysis as the right spot for judges to evaluate the policy trade-offs associated with surveillance strategies.

Survey data also can play a role in applying the "private-facts" model that would become the core of *Katz* prong 2 under our framework. Determining what information counts as sensitive requires numerous subjective judgments. Sensitivity depends a great deal on context, on the identity of the recipient of the information, on the preferences of the data privacy subject, the risks posed by present or future disclosure, and the priors of the person evaluating the information.[134] People and even cultures are heterogeneous with respect to what information about themselves they are willing to share, with

---

[130] The out-of-pocket cost for Wave 3 of our large-sample survey was $4,550, but that survey instrument was used to generate results relevant to four separate research papers by the authors. Obviously, this figure does not include the authors' imputed wages for designing the survey and analyzing the results.

[131] See, for example, *Grady v North Carolina*, 135 S Ct 1368, 1371 (2015).

[132] See note 71.

[133] Some readers and courts might prefer to see a purely normative judicial inquiry in *Katz* step 2 and the incorporation of survey data about sensitivity and embarrassment into the reasonableness inquiry. We think there is a case to be made for that approach instead of the one we advocate in the text. What we object to is redundant double-counting.

[134] See, for example, Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, 2009); Paul Ohm, *Sensitive Information*, 88 S Cal L Rev 1125 (2015).

whom they are willing to share it, and under what circumstances sharing is appropriate.[135] Differences in individuals' psychological worldviews contribute to this heterogeneity,[136] and the result is that it can be difficult to determine what counts as sensitive.

Yet this again leads us to public opinion data. Supreme Court cases are, as Kerr notes, inconsistent in their application of the private-facts model. Under that model, dog-sniff tests used to determine whether drugs are inside a tent or chemical tests that indicate whether a powder that has spilled outside a FedEx package en route do not amount to searches because all the tests do is help police sort between contraband and legal substances. The fact that an object is contraband is deemed nonsensitive.[137] But if the police open a package to determine its contents and find drugs inside or bring a drug-sniffing dog to someone's front porch, that *is* a search, with the private-facts model receiving little attention.[138] And if a police officer who is lawfully in a home nudges stereo equipment a few inches to see its serial number so he can check whether it has been reported stolen, that's a search, even though the serial number sought and seen is not sensitive.[139] The law's coherence is undermined by the fact that the cases variably veer between treating the sensitivity of the information sought as decisive and dismissing it as irrelevant.

Against this backdrop, a more objective and replicable way to address the question of sensitivity is to poll a representative sample of ordinary Americans and see what they say is sensitive in what context. Christopher Slobogin has shown exactly how this sort of research can be done, constructing a hierarchy of more- and less-sensitive data based on popular attitudes.[140] Taking a shortcut by substituting judicial hunches for the actual view of the populace seems

---

[135] See generally James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L J 1151 (2004); Adam M. Samaha and Lior Jacob Strahilevitz, *Don't Ask, Must Tell, and Other Combinations*, 103 Cal L Rev 919 (2015).

[136] Matthew B. Kugler, *Affinities in Privacy Attitudes: A Psychological Approach to Unifying Informational and Decisional Privacy*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2469562.

[137] Kerr, 60 Stan L Rev at 513–15 (cited in note 60) (discussing *United States v Jacobson* and *Caballes v Illinois*).

[138] Id at 515; *Florida v Jardines*, 133 S Ct 1409, 1417 (2013).

[139] *Arizona v Hicks*, 480 US 321, 325–26 (1987); Kerr, 60 Stan L Rev at 514–15 (cited in note 60).

[140] See, for example, Slobogin, *Privacy at Risk* at 110–13, 183–84 (cited in note 24).

particularly misguided. To be sure, there may be some easy cases where judges will conclude, uncontroversially, that information is highly sensitive (take social security numbers, for example[141]), but in these easy cases survey respondents will get the answer right too.[142] Contemporary polling on sensitivity produces a hierarchy that many readers will find intuitive. Americans regard social security numbers, a list of medications they take, and the contents of their phone conversations as highly sensitive, the list of websites they have visited and queries they have run in search engines as moderately sensitive, and their basic purchasing habits and the sort of media they like to consume as not terribly sensitive.[143] Some readers may prefer to construct the hierarchy differently than the median citizen does, but the popular consensus reflects a level-headed judgment about what sort of information would be dangerous to the individual if broadly disclosed and (relatedly) what sort of information most people tend to guard closely. The principles underlying popular attitudes are more readily comprehensible than those underlying the Court's private-facts cases.[144] In presenting this article, we sometimes get accused of over-privileging the naive priors of laypeople. But when the judgments of the crowd are placed alongside those of jurists, the crowd doesn't seem less wise. Of course one can quibble with majoritarian judgments. Perhaps survey respondents underestimate the threat that is associated with people knowing what websites they visit, but if so the federal courts have erred in the same way.[145]

---

[141] See, for example, *Greidinger v Davis*, 988 F2d 1344 (4th Cir 1993).

[142] See, for example, Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* at 7 (Nov 12, 2014), archived at http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (reporting that 90% of Americans surveyed describe their social security number as "very sensitive," a much higher rate than any other sort of information about which respondents were surveyed).

[143] Lee Rainie, *The State of Privacy in America: What We Learned*, Pew Research Center (Jan 20, 2016), archived at http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

[144] Indeed, the four dissenters in *Jardines* effectively point out the incoherence of the Court's conflicting approaches to dog sniffs. See *Florida v Jardines*, 133 S Ct at 1424–25 (Alito, J, dissenting). To make sense of the case law, it is necessary to either embrace a slippery act-omission dichotomy or make highly contestable assumptions about the dynamic effects of particular enforcement policies, along the lines of those suggested by Kerr, 60 Stan L Rev at 534–35 (cited in note 60).

[145] *See United States v Forrester*, 512 F3d 500, 510 (9th Cir 2008) (holding that there is no Fourth Amendment reasonable expectation of privacy in a list of IP addresses one has visited).

And here is the rub. We want law enforcement and security personnel to be able to assess the legality of such programs ex ante. Assessing the social welfare effects of a new investigative technique is even harder ex ante than it would be ex post, but decisions to greenlight an investigative strategy have to be made ex ante. Can a local police chief or CIA director commission a poll where she hires reputable survey researchers to figure out where public sentiment is on dozens of new investigative techniques that the department or agency is considering implementing? Yes, and she can do so on a tight budget these days. A good social scientist might be hired to design and run a survey for less than the price of ten or twenty outside counsel billable hours,[146] and if even that is too pricey our own aim is to collect lots of these data over time and make them freely available on the Internet. We provide some of these data in Table 9.

### D. HOW SURVEY RESEARCH CAN RESTORE COHERENCE TO KATZ DOCTRINE

This brings us to our final point before we dive into the data. Recall that the Supreme Court's *Katz* test is articulated as a two-prong inquiry—the courts are to look to subjective and objective expectations of privacy. Yet it appears that *Katz*'s subjective prong has atrophied. For this development, Orin Kerr blames a misreading of Justice Harlan's original *Katz* opinion by the Supreme Court in cases like *Smith v Maryland*, which articulated *Katz*'s subjective prong in terms of how much privacy a reasonable defendant would expect with respect to numbers he dialed into a land-line telephone's handset.[147] But what if there is a better way to be faithful to both *Smith* and the version of *Katz* that emerged from *Jones*?

Integrating *Smith v Maryland* with *Jones*, one could instead apply the *Katz* test in three steps. Beginning with *Katz*, through the lens of *Jones*, one would ask whether police conduct infringed on a suspect's property right. If the police committed a trespass, then the conduct amounts to a search and the courts need only ask whether

[146] The authors would like to conduct surveys like the ones we describe in this article on an annual basis and to make the results of our surveys available online for free. To the extent that courts begin relying on survey data in Fourth Amendment contexts, we would expect other academic survey researchers to launch similar efforts, creating a large repository of current public domain opinion research. See note 113.

[147] See Kerr, 82 U Chi L Rev at 128–33 (cited in note 59).

the warrantless search was reasonable. Second, assuming there was no trespass, a court would apply *Katz*'s two traditional prongs. For prong 1, it would examine whether privacy was expected in a particular situation. Because getting inside the defendant's head is neither easy nor helpful, and it will always be tempting for a defendant to claim falsely (for the benefit of an evidentiary motion) that he did, in fact, expect privacy,[148] the law should use the sentiments of the median American citizen as a proxy for the defendant's subjective expectation of privacy. If more Americans would have expected privacy in a particular situation than not, it is reasonable to assume that the defendant did too. Arguably even a lower threshold should be used, or courts could allow some consideration of heterogeneous privacy expectations across race and gender lines.[149]

Assuming the police acted in a way contrary to the expectations of the median American or the median American of a protected class, the court would shift its attention to *Katz*'s second prong—whether the defendant's subjective expectation of privacy is one society is prepared to accept as reasonable. Because *Jones* moved the "positive law" inquiry outside of *Katz* and our doctrinal suggestion moves the "probabilistic" model from *Katz* prong 2 to *Katz* prong 1, the second

---

[148] It is perhaps puzzling why the law should care inherently about the individual defendant's actual expectation of privacy. Given that courts articulate precedents that guide thousands of people who will never litigate, a generally applicable inquiry into whether most people actually would have expected privacy in a (recurring) circumstance is more helpful. From an ex ante perspective, improving the alignment between the law and expected outcomes reduces the costs associated with learning the law and modifying one's behavior. See notes 88–89 and accompanying text.

[149] One might argue that if most members of a minority group would expect privacy in a particular setting, then *Katz* prong 1 should be satisfied regardless of whether a particular defendant happens to be a member of that minority. In our data set, neither race nor gender has any measurable association with privacy expectations toward GPS tracking. But we can imagine situations in which race or gender could influence peoples' expectations, and in those instances society might want to make sure that the law protects potentially marginalized subgroup members. A good example is *Safford Unified School District #1 v Redding*, 557 US 364 (2009), a case involving a school's search of a thirteen-year-old girl's undergarments. Justice Ginsburg has said that during the Justices' arguments about the case, she was able to convince her colleagues that a thirteen-year-old girl has different concerns and expectations about being forced to remove her clothes than a thirteen-year-old boy. See Emily Bazelon, *The Place of Women on the Court*, NY Times MM22 (July 7, 2009). To do that in a manner consistent with the Fourteenth Amendment, Fourth Amendment doctrine likely needs to protect everyone. The existence of privacy expectations among some oddly configured and obscure subgroup—say, Buddhist soccer moms in suburban Nebraska—would be insufficient to create reasonable expectations of privacy for everyone. Were it otherwise, then data miners could always satisfy our *Katz* prong 1 test. Moreover, law enforcement cannot be required to anticipate every obscure subgroup's prevalent privacy expectations. For those reasons, a court open to minoritarian expectations of privacy might focus on categories like race and gender.

prong of *Katz* now gives the courts an opportunity to consider the "private-facts" model. Courts must have a sense of what information is considered "private" to assess whether a particular technique implicates sensitive "private facts."

We think this approach is basically what the Supreme Court was trying to do in *Smith v Maryland*,[150] though the Court's execution left much to be desired. In *Smith* the issue before the Court was whether law enforcement's use of a pen register to record all the numbers dialed on a suspect's phone amounted to a search. The Court began by examining *Katz*'s first prong. As the Court saw it:

> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. . . . Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[151]

The Court recognizes the difficulty of figuring out what Smith thought, so it pivots to the question of what people in general think about the privacy of call information.[152]

Counsel for Smith argued to the Court that regardless of what "telephone users in general" thought when they dialed their numbers, Smith himself expected privacy because he placed the call from inside his residence.[153] The Court rejected this argument too,

---

[150] 442 US 735 (1979).

[151] Id at 742–43.

[152] To be sure, its empirical intuitions were likely off-base. It cited no evidence for its broad assertions about what "all telephone users" and "most people" believed in the 1970s, and some of its factual inferences seem to assume a higher level of sophistication than ordinary Americans typically possess. See *Smith*, 442 US at 748–49 & n 1 (Marshall dissenting). The Court played fast-and-loose with some facts. The majority notes that the phone call at issue was a local call, not a long-distance call. Given that many Americans at the time paid a flat monthly fee for local calls and saw no itemized bills for them, it is possible that many Americans would have believed the phone company kept no records of outgoing calls.

[153] Id at 743.

once again drawing on the views of telephone users in general to do so. As the Court wrote, "Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would."[154] With this sentence, the Court indicated that it hardly cared what Smith himself thought.[155] A rational subscriber could not expect that the numbers he dialed would remain private, so Smith would still lose under prong 1. The Court then noted that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private," such an expectation would not satisfy *Katz*'s objective prong.[156]

In summary, then, we believe there is a good case to be made for interpreting Fourth Amendment law in a manner consistent with *Smith v Maryland* but in some tension with other pronouncements by the Court. Rather than throwing overboard the first prong of *Katz*'s canonical test, as many courts seem to be doing,[157] we would propose resuscitating it by making popular expectations an important part of the inquiry into whether an individual maintained reasonable expectations of privacy in a particular setting. The costs of obtaining reliable evidence about such expectation have fallen dramatically, and with those diminished costs come increased predictability. Under our approach, popular sentiment gauged by reliable social science methods would become a necessary (though not sufficient) element of a court's determination that a particular investigative technique amounted to a search. If survey results suggested that the use of technology violated people's expectations, then the courts would turn to an examination of the sensitivity of the information sought and obtained.

We want to make two final points before concluding this part. First, there will surely be some overlap between expectations and sensitivity. Police surveillance into the interior of a home is deeply

[154] Id.

[155] See also note 148.

[156] Id.

[157] See Kerr, 82 U Chi L Rev at 131 (cited in note 59).

troublesome to people both because of what the investigation looks like and what it reveals. Indeed, it is very interesting that while both Justice Alito and Justice Sotomayor arguably embraced the mosaic theory in *Jones*, Alito focused on popular expectations in his articulation of the mosaic theory and Sotomayor emphasized the sensitivity of the information gathered through long-term surveillance.[158]

Second, though both our approach and Slobogin's approach are driven by survey data, we use these data in different ways. Slobogin uses survey results to assemble a hierarchy of searches, scaled to the perceived intrusiveness of the search, and then balances the proportional costs of that intrusiveness against the security benefits of the surveillance.[159] His surveys invite normative judgments on the part of laypeople, and some subsequent researchers have done likewise.[160] We, by contrast, are primarily asking for descriptive assessment by laypeople—how unexpected would this be?—and then sliding their responses into the existing *Katz* framework for determining the Fourth Amendment's scope. So while there are important commonalities and areas of agreement, we are collecting more representative data, about different questions, and putting those data to a divergent doctrinal use. That said, we think a data-driven approach to determining sensitivity—along the lines suggested by Slobogin—would represent an improvement on current practice. In part to promote dialogue between his approach and ours, we asked the traditional Slobogin intrusiveness question in Wave 3 and describe how it relates to the expectation data in Part III.E.

Having made the case for survey research's relevance, we will now present the results of our research into the public's attitudes regarding the key doctrinal issue left open by *United States v Jones*. When law enforcement obtains geolocation information from a criminal suspect without effecting a trespass onto land or chattels, how long can the surveillance continue before a warrant is required?

---

[158] Compare *Jones*, 132 S Ct at 962–63 (Alito, J, concurring), with *Jones*, 132 S Ct at 955–56 (Sotomayor, J, concurring).

[159] Slobogin, *Privacy at Risk* at 180–96 (cited in note 24).

[160] See Scott-Hayward et al, *Does Privacy Require Secrecy?* at 39–40 (unpublished) (cited in note 113).

## III. Empirical Data about Views on Surveillance Duration

So far we have shown how public opinion surveys can help resolve Fourth Amendment questions about what constitutes a search. Hard data about Americans' expressed beliefs are highly relevant to the constitutional inquiry. The data could be decisive in some cases. But this raises an obvious problem. What if the American people are as divided as the lower courts over the question of duration salience? Happily, it turns out that American citizens have coalesced around two clear points of consensus. First, the duration of geolocation tracking strikes the lion's share of Americans as irrelevant to the question of whether a reasonable expectation of privacy has been violated. Second, Americans are nearly two and a half times more likely to view geolocation surveillance of any duration as infringing a reasonable expectation of privacy as they are to reach the opposite conclusion.

### A. Participants, Procedure, and Measures for Waves 1 and 2

A weighted sample of adult Americans was recruited by Toluna, a professional survey firm with an established panel.[161] The sample was drawn to mirror closely the American population as a whole across various demographic dimensions.[162] The panel was recruited in two waves but, as there are no differences between waves on any of the relevant measures, the results are combined for most of

[161] For discussion of demographically weighted panels and online versus telephone surveys, see generally J. Michael Brick, *The Future of Survey Sampling*, 75 Pub Opinion Q 872, 881–85 (2011); Dan Farrell and James C. Petersen, *The Growth of Internet Research Methods and the Reluctant Sociologist*, 80 Sociological Inquiry 114, 116–20 (2010); Robert P. Berrens et al, *The Advent of Internet Surveys for Political Research: A Comparison of Telephone and Internet Samples*, 11 Pol Analysis 1, 5–21 (2003).

[162] The sample was 51.3% female; 80.6% of the sample identified as White, 11.5% as Black, and 4.6% as South or East Asian. On a separate question, 16.7% reported identifying as Hispanic or Latino. The median age was 51 (range 18–95, $M = 48.56$, $SD = 16.80$). On a scale ranging from 1 (very liberal) to 7 (very conservative), the mean response was 4.23 ($SD = 1.72$), indicating a politically moderate sample. Slightly more of the sample than the national population as a whole had completed at least some college coursework. In the sample, 14.1% had graduate degrees, 28.7% had four-year college degrees, 23.3% had two-year degrees, 32.2% had high school degrees, and 1.6% had not completed high school. According to the U.S. Census Bureau, 12.7% of those 35–39 have graduate degrees, a further 22.6% have four-year degrees, 10.8% have two-year degrees, 42.8% have a high school degree but have not completed any college degree, and 11.2% do not have a high school degree. See United States Census Bureau, Educational Attainment in the United States: 2012—Detailed Tables, archived at http://www.census.gov/hhes/socdemo/education/data/cps/2012/tables.html.

our data analysis.[163] The final sample contained 1,461 participants, all of whom were adult U.S. citizens.[164]

For the key question, participants were asked, Would it "violate people's reasonable expectations of privacy if law enforcement" (1) used a car's onboard GPS system to locate it on public streets without the owner's permission? (2) used a car's onboard GPS system to track its movements on public streets for one day without the owner's permission? (3) same, but for one week? (4) same, but for one month?

Participants answered these four questions on response scales that ranged from 1 (definitely not) to 5 (definitely yes). The questions asked about the use of a car's own GPS system—rather than a GPS tracking device installed by police—to better reflect the types of nontrespass cases that have arisen in the wake of *Jones*.[165]

### B. MAIN RESULTS

The participants were more likely than not to believe that this type of GPS tracking violated reasonable expectations of privacy. As can be seen in Table 1, roughly twice as many participants scored above rather than below the scale's midpoint on each question. Also, the response mean was significantly above the scale's midpoint for each of the four questions.[166] These data therefore provide a clear answer to whether GPS tracking violates reasonable expectations of privacy in the eyes of ordinary citizens.

In addition to this baseline expectation of privacy, there was a small yet discernible effect of tracking duration.[167] People were more

[163] Wave 1 data were gathered June 11–12, 2014. Wave 2 data were gathered July 1–2, 2014. There were differences between these waves on other measures, but those differences are not relevant to this project.

[164] The survey instrument contained a question directing participants to show that they were paying attention by selecting a particular answer choice. Only participants who responded correctly to this question were included in the analysis.

[165] See notes 31–44 and accompanying text. We avoided asking about the duration of geolocation tracking via cell-phone towers because we knew the *Riley* case, involving the privacy of cell-phone contents when the phone's owner is arrested, would be decided between Wave 1 and Wave 2.

[166] One-sample *t*-tests revealed that all mean scores were significantly above the scale's midpoint value of 3. The *t*-values for locate, one day, one week, and one month were 10.29, 13.42, 14.48, and 15.41, respectively. All are significant at $p < .001$.

[167] A mixed analysis of variance was conducted to examine whether there were consistent differences between participants' responses to the four GPS tracking questions. There were

Table 1
Effect of Duration on Privacy Expectation

| | *M* | *SD* | % Below Midpoint | % Above Midpoint |
|---|---|---|---|---|
| Locate | 3.41 | (1.51) | 28 | 51 |
| Track 1 day | 3.53 | (1.51) | 25 | 56 |
| Track 1 week | 3.57 | (1.51) | 25 | 58 |
| Track 1 month | 3.61 | (1.51) | 24 | 59 |

NOTE.—Responses were on a 1–5 scale with higher values corresponding with greater invasion of privacy. All pairwise comparisons are significant.

inclined to say that a person's reasonable expectation of privacy is violated by month-long tracking than by week-long, more by week-long than day-long, and more by day-long than instantaneous.[168]

This effect of duration on expectations hides an underlying consistency in responses across measure. Most participants give the same response to each of these four questions, and only a handful show the kind of rising trend pattern implied by the gradually increasing means. As can be seen in Table 2, nearly 40% of respondents consistently reported that people's expectations of privacy would be violated in all these situations (giving ratings of all fours or all fives).[169] A further 16.9% consistently reported that they believed expectations of privacy were not violated (all ones or all twos), and 11% consistently gave the middle response (all threes). Only 5.3% gave responses that started low—stating that expectations of privacy were not violated—and ended high. This is the pattern of responses that would be consistent with Justice Alito's view in *Jones* that surveillance duration is highly salient, and it was nearly eight times less popular than the view that all durations of geolocation tracking equally violate people's expectations of privacy.

The "none of these patterns" category represents a puzzle. A portion of the respondents in that category appeared to be particularly sensitive to the use of a GPS device to determine where a

no effects of wave and no interaction between wave and duration. Wave $F(1, 1459) = .82$, $p = .37$; interaction $F(1.98, 2884.80) = .16$, $p = .85$. A Greenhouse-Geisser correction was used for the within-subjects portion of this analysis because Mauchly's test revealed a sphericity violation.

[168] $F(1.98, 2884.80) = 33.62$, $p < .001$, $\eta 2 = .023$. All pairwise comparisons are significant at the $p < .05$ level.

[169] Fully 45.4% of respondents gave only fours or fives (in some combination) on this question, versus 19% who gave only ones or twos. This is a 2.39:1 ratio.

Table 2
Patterns of Privacy Responses

| Response | % |
|---|---|
| Consistently high | 39.5 |
| Consistently middle | 11.0 |
| Consistently low | 16.9 |
| Rising trend that does not cross midpoint | 11.8 |
| Rising trend that crosses the midpoint | 5.3 |
| None of these patterns | 15.5 |

NOTE.—Proportion of participants using each of the above response patterns.

vehicle is *right now*, reporting a high level of privacy invasion for that item and lower scores for longer duration monitoring. Others may have believed that long-term tracking would necessarily be less granular than short-term tracking, or simply been confused. The study was not designed to differentiate between these perspectives, so we cannot make any definitive statement about what was driving these relatively rare responses.

The level of consistency appears to be even higher if one looks question by question. Table 3 reports the percentage of people giving the same response to each possible pair of questions. Obviously there is more consistency between neighboring questions—locate is closer to one day than to one week, etc.—but the general theme is one of extreme consistency. As mentioned above, most courts that have tried to draw a duration distinction have put the line somewhere between a day and a month. Here, more than 81% of respondents gave the same scores to month- and day-long tracking. The expectations judgment, then, appears to be qualitative rather than quantitative: conduct is a search, or it is not. Duration is largely irrelevant.

In a follow-up study (reported in the Online Supplement OS.A), we tested variants of the question reported here that altered both the question text, whether it asked about "expectations of privacy," "reasonable expectations of privacy," or merely "privacy," as well as whether the question referred to "people's" privacy versus "your" privacy. The changes in privacy wording had no effect on the pattern of consistency reported above.[170] We therefore have reason to believe that our results are robust to minor variations in question

[170] The use of first-person wording only had the effect of slightly elevating privacy expectations across the board. This is consistent with a similar effect reported by Slobogin

Table 3
Percentage of Respondents Whose Scores Are Identical Across Question Pairs

| | 1 Day (%) | 1 Week (%) | 1 Month (%) |
|---|---|---|---|
| Locate | 77.9 | 72.4 | 71.6 |
| 1 day | | 83.4 | 81.2 |
| 1 week | | | 91.2 |

wording. We also observed that the sample in that follow-up study, which was from Amazon's Mechanical Turk rather than a representative sample like the ones reported above, was substantially more privacy protective.[171] This leads us to be very concerned about the use of Mechanical Turk to establish base rates in this type of privacy research.

### C. EXPLANATIONS

Respondents in Wave 2 who reported consistently low or consistently high privacy expectations were asked to report their reasoning on a subsequent page. This page noted that the participants had given consistent responses and gave a list of reasons that would support their doing so. They were asked to select the best one or two of the provided answers, or to contribute their own.

To our surprise, the dominant option among the minority who reported consistently low expectations of privacy is an articulation of the third-party doctrine: the car's driver is sharing the information of their location with a number of parties and, as such, assumes the risk that it will be shared with the government (see Table 4). As

and Schumacher, 42 Duke L J at 759 (cited in note 92). First- versus third-person wording did not affect the consistency pattern.

[171] The nationally representative sample gave mean expectation ratings for locate, one day, one week, and one month searches of 3.41, 3.53, 3.57, and 3.61, respectively (Table 1). The same numbers for the identically worded question (third person, reasonable expectations) from the Mechanical Turk collection were 4.02, 4.22, 4.32, and 4.35, respectively, an average difference of .70 on a five-point scale. To give some sense of magnitude, .70 is also roughly the difference in expectation ratings we observe between examining the content of a person's emails and inspecting a hotel guest registry (see Table 9). Similarly, the proportion of people with consistently high responses goes from 39.50% to 49.20%, while the proportion with consistently low responses goes from 16.90% to 5.88%. See also Ruogu Kang et al, *Privacy Attitudes of Mechanical Turk Workers and the U.S. Public*, USENIX Association Tenth Symposium on Usable Privacy and Security 37, 42 (2014), archived at https://www.usenix.org/system/files/conference/soups2014/soups14-paper-kang.pdf.

Table 4
Reasons Given by Those with Consistently Low Privacy Expectations (16.9% of the Sample)

| Reason | % |
|---|---|
| The driver of the car is already sharing the information from the GPS with several companies (e.g., OnStar, the car manufacturer, the company that owns the GPS satellites, etc.) so the driver should expect that the same information can be shared with law enforcement. | 65.19 |
| A car is being driven on public roads, so any police car in the vicinity already could lawfully determine a car's location or even follow the car for a month. | 29.63 |
| It is very important that the police be able to keep the population safe, and privacy interests should give way to public safety interests. | 25.19 |
| Only sensitive information like medical history, sexual behavior, or political beliefs should be private and someone's whereabouts during a particular day or month isn't sensitive. | 20.00 |
| Dangerous driving is an activity that puts others' lives at risk, and cars are often used to commit crimes, so drivers should not expect any privacy behind the wheel. | 20.00 |
| Privacy is a relic of the past. In 2014, people really should not expect privacy in any settings, especially when technology is involved. | 17.04 |
| Other | 6.67 |

NOTE.—Numbers display the percentage of participants selecting each of the available options. Participants were asked to select the best one or two options, but were not prevented from checking more than two boxes.

it has been applied by the courts, the third-party doctrine has been routinely attacked for not being consistent with everyday understandings of privacy.[172] It is therefore particularly interesting to see that most of those who express low privacy expectations actually do cite it as a driving force in their analysis. Less than half as many participants cite the explanation that the authors would have predicted: that the car is visible on public roads and could be monitored there by other means. This type of reasoning, suggestively endorsed by the Supreme Court in *United States v Karo*,[173] played a distinct second fiddle to the unexpectedly popular third-party doctrine. Other plausible theories did not attract high levels of support.

[172] See, for example, Slobogin and Schumacher, 42 Duke L J at 734, 740 (cited in note 92); Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 Harv J L & Tech 199, 214–15 (2011); see also sources cited note 20.

[173] 468 US 705, 717–19 (1984).

Two concerns predominated among those who consistently exhibited high privacy expectations: (1) that the police would abuse GPS tracking if they were free to use it, and (2) that even locating a car through GPS tracking imposes substantial restrictions on personal freedom (see Table 5). The first of these concerns does not directly speak to privacy expectations and may indicate a general discomfort with granting the police the power to invade the privacy of citizens absent some type of process. The second echoes part of the concern expressed by Justice Sotomayor: that monitoring of GPS information is not harmless and may chill certain types of lawful behaviors.[174]

One theory rejected by these respondents was that the sheer impracticality of locating or tracking a random vehicle in a pre-GPS world—requiring a huge investment of resources—makes the tracking unexpected. Lest this idea be dismissed as an obvious straw man, consider Justice Sotomayor's view that long-standing resource constraints on government investigations continue to inform reasonable expectations of privacy,[175] and Justice Alito's discussion of the "very tiny constable" needed for eighteenth-century carriage tracking.[176] There is something appealing in the theory that it violates people's privacy expectations when law enforcement acquires a seemingly magical new ability to gather information about the activities of the citizenry. Yet less than 10% of even privacy-conscious participants think in those terms.

### D. PERSONALITY DIFFERENCES

We approach the issue of Fourth Amendment law with a particular interest in the psychological underpinnings of privacy sentiment. Scholarly understandings of the psychology of privacy are in their infancy, and there have been only a few papers considering whether people with strongly protective privacy views are system-

---

[174] *Jones*, 132 S Ct at 955 (Sotomayor, J, concurring).

[175] Id at 956 (Sotomayor, J, concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques . . . it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources . . .'").

[176] In the majority, Justice Scalia analogized the state's action in *Jones* to "a constable's concealing himself in the target's coach in order to track its movements," which would amount to trespassing. 132 S Ct at 950 n 3. Justice Alito appeared to find this risible. See id at 958 n 3 (Alito, J, concurring) ("[T]his would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.").

Table 5
Reasons Given for Consistently High Privacy Expectations (39.5% of the Sample)

| Reason | % |
|---|---|
| If the police could do this to anyone at any time they would very likely abuse the power. | 58.74 |
| It really restricts personal freedom for the police to be able to locate a car whenever they feel like it, and that kind of privacy shouldn't be compromised. | 54.55 |
| It is wrong for the police to use a person's own GPS system to track them because it is their own property. | 35.31 |
| The police might learn just as much about a person from one day's monitoring as from one month's, so they're both equally intrusive. | 21.33 |
| Privacy interests are very important, and public safety interests should always give way to them. | 19.58 |
| The police could not track a car's location using officers in squad cars without spending lots of resources, so people don't expect it. | 9.79 |
| Other | 4.20 |

NOTE.—Numbers display the percentage of participants selecting each of the available options. Participants were asked to select the best one or two options, but were not prevented from checking more than two boxes.

atically different than others.[177] Our survey instrument therefore contained several measures that are useful for mapping the effects of personality and political ideology on privacy attitudes. Results on some of these are reported here (see Table 6), and the rest are included in the Online Supplement OS.D. We analyzed responses using a between-subjects analysis of variance with the response categories described in Table 2 as the between-subjects factor.

The two most interesting effects we discovered were on age and authoritarian submission. The age effect was very simple: those in the low privacy expectation group were significantly older on average than people in the other three groups.[178] This was a moderate effect, with the difference between the consistently high and consistently

[177] See Sunil Hazari and Cheryl Brown, *An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites*, 9 J Info Privacy & Security 31, 41–45 (2013); Deborah M. Moscardelli and Richard Divine, *Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors*, 35 Family & Consumer Science Res J 232, 243–47 (2007); Mike Z. Yao, Ronald E. Rice, and Kier Wallis, *Predicting User Concerns about Online Privacy*, 58 J Am Soc Information Science & Tech 710, 718–20 (2007); Hoofnagle and Urban, 49 Wake Forest L Rev at 261 (cited in note 112); Kugler, *Affinities in Privacy Attitudes* (unpublished) (cited in note 136); Alan F. Westin, *"Whatever Works": The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, in *Privacy and Self-Regulation in the Information Age* ch 1, § F (1997), archived at http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

[178] All post-hoc tests described as significant are significant at least at the $p < .05$ level.

Table 6
Personality Characteristics as a Function of Privacy Views

| | $F$ (3,1229) | $\eta^2$ | Consistently High | Consistently Low | Consistently Middle | Rising Trend |
|---|---|---|---|---|---|---|
| Liberalism-conservatism | 1.23 | .003 | 3.95 (1.70) | 4.18 (1.75) | 4.08 (1.51) | 3.99 (1.63) |
| Authoritarianism | 11.95*** | .028 | $3.50_{c}$ (1.04) | $3.94_{a}$ (.98) | $3.60_{bc}$ (.73) | $3.67_{b}$ (.92) |
| Age | 8.84*** | .021 | $47.58_{b}$ (16.59) | $54.00_{a}$ (16.21) | $48.97_{b}$ (16.44) | $49.62_{b}$ (16.36) |
| Supreme Court knowledge | .87 | .002 | .51 (.33) | .53 (.33) | .48 (.32) | .52 (.33) |

NOTE.—Group means are significantly different when they do not share subscripts. So for authoritarianism, the consistently high group (c) is significantly different than the low group (a) but not the middle group (bc).

*** $p < .001$.

low group means amounting to 6.42 years. This finding cuts strongly against the conventional wisdom that younger cohorts do not care about their privacy.[179]

Authoritarian submission requires a word of explanation. The social psychological theory of authoritarianism defines authoritarians as people who are especially willing to submit to authority, who believe that it is particularly important to yield to traditional conventions and norms, and who are hostile and punitive toward those who question authority or who violate such conventions and norms.[180] The Authoritarian Submission Scale, developed by John Duckitt and colleagues, is intended to measure the first of those impulses: the extent to which people believe that authority should be respected and obeyed rather than challenged and questioned.[181] Authoritarianism is one of the two major individual difference constructs in political psychology.[182] It has been shown to correlate with attitudes toward a wide array of political issues, including abortion, affirmative action, racial minorities in general, illegal drug use, the homeless, homosexuality, and, among men, hostility toward women.[183]

---

[179] See, for example, Teri Dobbins Baxter, *Low Expectations: How Changing Expectations of Privacy Can Erode Fourth Amendment Protections and a Proposed Solution*, 84 Temple L Rev 599, 609–14 (2012); Jo Bryce and Mathias Klang, *Young People, Disclosure of Personal Information and Online Privacy: Control, Choice, and Consequences*, 14 Info Sec Technical Rep 160, 160 (2009) ("It has been claimed that users, particularly young people, have a lack of interest in their online privacy. . . ."). But see Moscardelli and Divine, 35 Family & Consumer Science Res J at 246 (cited in note 177) (finding teens had higher levels of privacy vigilance than adults, as reflected on temporally distant survey responses); Chris Jay Hoofnagle et al, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* at ∗20 (unpublished article April 14, 2010), archived at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 (finding younger respondents and older respondents largely in alignment with respect to privacy attitudes and concerns).

[180] See Bob Altemeyer, *The Other "Authoritarian Personality,"* in Mark Zanna, ed, 30 *Advances in Experimental Social Psychology* 47–92 (Elsevier, 1998).

[181] Items include "It's great that many young people today are prepared to defy authority" (reverse coded), and "What our country needs most is discipline, with everyone following our leaders in unity." The response scale ranged from 1 (strongly disagree) to 6 (strongly agree). Higher scores indicate stronger endorsement of authoritarian ideologies. John Duckitt et al, *A Tripartite Approach to Right-Wing Authoritarianism: The Authoritarianism-Conservatism-Traditionalism Model*, 31 Pol Psych 685–715 (2010). The other two authoritarianism scales developed by Duckitt and colleagues (authoritarian aggression and traditionalism) were also administered. We believe that authoritarian submission is a better measure of the ideology construct for these purposes, however.

[182] See generally John Duckitt and Chris G. Sibley, *A Dual Process Motivational Model of Ideological Attitudes and System Justification*, in John Jost et al, eds, *Social and Psychological Bases of Ideology and System Justification* 292 (2009); Altemeyer, *The Other "Authoritarian Personality"* at 47 (cited in note 180).

[183] Herbert L. Mirels and Janet B. Dean, *Right-Wing Authoritarianism, Attitude Salience, and Beliefs about Matters of Fact*, 27 Political Psych 839, 840–41 (2006) (reviewing studies).

The effect on authoritarian submission was similar to that on age: those with consistently low privacy expectations had significantly higher authoritarianism scores than those in any other category. The difference between the consistently high and consistently low groups was moderate, amounting to about half a standard deviation. These results are supported by prior work showing that those high in authoritarianism are consistently less supportive of both information and decision privacy protections.[184] In fact, the same Authoritarian Submission Scale has previously displayed a moderate correlation with a composite of criminal procedure privacy questions.[185]

Two other interesting factors did not differ across condition. First, there was no overall effect of political orientation. Despite the authoritarianism finding, those with lower privacy expectations did not tend to be more conservative. Second, Supreme Court knowledge, assessed with a four-question quiz, also had no effect.[186]

Our surprising finding about age has important implications for judicial behavior. Judges tend to be much older than the population at large. This means that the group entrusted with actually assessing expectations of privacy is unrepresentative on an important dimension. And those who endorse the third-party doctrine are significantly older than even others with low privacy expectations.[187] This disproportionate appeal of the third-party doctrine to older Americans could help explain its persistence in legal doctrine despite its apparent lack of resonance with younger Americans.

### e. wave 3: replication, intrusiveness, and suggestive data on other searches

A third wave of data was collected between May 26 and June 2, 2015, approximately a year after Waves 1 and 2. Participants for this wave were also recruited by Toluna. The final sample con-

---

[184] See Kugler, *Affinities in Privacy Attitudes* (unpublished) (cited in note 136). This result may reflect the historical links between privacy protections and autonomy beliefs. Louis Henkin, *Privacy and Autonomy*, 74 Colum L Rev 1410, 1425 (1974).

[185] See Kugler, *Affinities in Privacy Attitudes* (unpublished) (cited in note 136). Table 3 of that paper shows a correlation of .37 between the criminal procedure composite and authoritarian submission. Importantly, the previous research in this area concerned privacy *attitudes* rather than privacy *expectations*. We suspect this difference in question type explains why the relationship between authoritarianism and privacy attitudes was stronger in the preceding paper.

[186] This is described in greater detail in the Online Supplement OS.D.

[187] $F(1,133) = 7.66$, $p = .006$, $\eta 2 = .054$. Endorse third-party doctrine ($M = 58.45$ years old, $SD = 15.62$). Low privacy expectations but adopting other theories ($M = 50.57$, $SD = 16.02$)

tained 1,441 respondents, all of whom were adult U.S. citizens. The demographic breakdown was similar to that in the first two waves.[188] Participants in this study received one of four versions of the GPS tracking question. One version mirrored that used in Waves 1 and 2 in that it asked about reasonable expectations of privacy and provided participants with a five-point response scale. The new wave employed a slightly revised version of the locate question.[189]

The results of each wave are nearly identical; there are no significant differences in the means or the consistency categories (see Table 7A and Table 7B). Even after a year, a year that included any number of events arguably relevant to police-community relations,[190] almost nothing had changed. These data should therefore help alleviate concerns that privacy expectations be inconsistent over time.

The second version of the GPS tracking question asked three questions designed to assess the intrusiveness of GPS tracking rather than expectations. For each search duration, participants were asked to rate the intrusiveness, the likelihood the search would reveal sensitive information, and how embarrassing the search would be (see Table 8).[191] The intrusiveness question mirrors that used by Slobogin in his research. The separate questions involving the revelation of personal information and embarrassment are intended to be supplemental measures of the social cost of allowing a search. They are drawn from Kugler's prior work on searches of electronic devices.[192]

---

[188] Of the sample, 49.8% was female; 12.1% had graduate degrees, 28.2% had four-year college degrees, 23.1% had two-year degrees, 34.5% had high school degrees, and 2% had not completed high school; 79.7% of the sample identified as White, 13.1% as Black, and 4.2% as South or East Asian. On a separate question, 17.1% reported identifying as Hispanic or Latino. The median age was 46 (range 18–89, $M = 46.04$, $SD = 16.41$). On a scale ranging from 1 (very liberal) to 7 (very conservative), the mean response was 4.19 ($SD = 1.78$).

[189] It now reads "Used a car's onboard GPS system to locate it on public streets without the owner's permission?" We believe this is clearer than the previous version. Both versions were used in the wording test study reported in the Online Supplement OS.A, and the results did not differ.

[190] See, for example, Michael S. Schmidt and Matt Apuzzo, *South Carolina Officer Is Charged with the Murder of Walter Scott*, NY Times A1 (April 8, 2015).

[191] "If law enforcement used a car's onboard GPS system to locate it on public streets at a single moment in time without the owner's permission: How intrusive would this be? How likely would this be to reveal sensitive personal information? How embarrassing would this be?" All response scales ranged from 1 (not at all) to 5 (very), with no labels on the other points. Note that the midpoint is less inherently meaningful for these three questions. Whereas a below-midpoint answer to the expectation question can fairly be read as "not violating expectations," a below-midpoint response to the embarrassment item may be fairly read as "only somewhat embarrassing."

[192] See Kugler, 82 U Chi L Rev at 1194 (cited in note 92) (using these as measures of the privacy and dignity interests implicated by border searches of electronic devices).

Table 7A
Categorical Consistency Between 2014 and 2015 Waves

| | Waves 1 and 2 (%) | Wave 3 (%) |
|---|---|---|
| Consistently high | 39.5 | 37.8 |
| Consistently middle | 11.0 | 11.0 |
| Consistently low | 16.9 | 15.2 |
| Rising trend/not cross | 11.8 | 13.5 |
| Rising trend/cross | 5.3 | 6.4 |
| None of these patterns | 15.5 | 16.0 |

Table 7B
Distributional and Mean Consistency Between 2014 and 2015 Waves

| | Waves 1 and 2 | | | Wave 3 | | |
|---|---|---|---|---|---|---|
| | *M* | % Below | % Above | *M* | % Below | % Above |
| Locate | 3.41 (1.51) | 28 | 51 | 3.44 (1.50) | 27 | 54 |
| Track 1 day | 3.53 (1.51) | 25 | 56 | 3.55 (1.52) | 24 | 57 |
| Track 1 week | 3.57 (1.51) | 25 | 58 | 3.67 (1.46) | 21 | 61 |
| Track 1 month | 3.61 (1.51) | 24 | 59 | 3.73 (1.46) | 19 | 63 |

NOTE.—Numbers in parentheses are standard deviations.

These data followed a somewhat different pattern in that there are larger shifts as the search duration lengthens. Though the expectation score increases by only .29 as the search lengthens from locate to 1 month, the intrusiveness score increases by .57, the sensitive information score by .61, and the embarrassment score by .45.[193] To the extent that the mosaic theory resonates at all with the public, that resonance has to do with the private-facts model and sensitivity, as Justice Sotomayor suggested, not the probabilistic model and expectations, as Justice Alito argued.[194] In our framework, surveillance duration is somewhat relevant under *Katz* prong 2 and irrelevant under *Katz* prong 1.

[193] This difference is reflected in the effect sizes for each measure. ANOVAs examining the effect of duration on expectations showed an effect size of only .048; $F(2.12, 765.77) = 18.02$, $p < .001$, $\eta 2 = .048$. The effect sizes for intrusion (.127), information (.127), and embarrassment (.090) were much higher: $F(2.14, 802.27) = 54.60$, $p < .001$, $\eta 2 = .127$; $F(1.92, 719.21) = 54.48$, $p < .001$, $\eta 2 = .127$; and $F(2.18, 815.45) = 36.98$, $p < .001$, $\eta 2 = .090$, respectively. Greenhouse-Geisser corrections used for all degrees of freedom.

[194] See note 158 and accompanying text.

Table 8
Mean Intrusiveness, Information, and Embarrassment Scores for Each Duration of Search

| | *M* | % Below | % Above |
|---|---|---|---|
| Intrusiveness: | | | |
| Locate | 3.59 (1.38) | 22 | 56 |
| Track 1 day | 3.95 (1.28) | 15 | 69 |
| Track 1 week | 4.07 (1.26) | 12 | 72 |
| Track 1 month | 4.16 (1.23) | 12 | 76 |
| Reveal sensitive information: | | | |
| Locate | 3.37 (1.33) | 25 | 47 |
| Track 1 day | 3.66 (1.22) | 17 | 56 |
| Track 1 week | 3.86 (1.21) | 13 | 63 |
| Track 1 month | 3.98 (1.20) | 12 | 70 |
| Embarrassment: | | | |
| Locate | 3.34 (1.36) | 25 | 45 |
| Track 1 day | 3.51 (1.30) | 20 | 50 |
| Track 1 week | 3.66 (1.30) | 18 | 55 |
| Track 1 month | 3.79 (1.32) | 16 | 60 |

NOTE.—Numbers in parentheses are standard deviations. Results in terms of the consistency categories are in the Online Supplement OS.C.

The final two versions of the GPS tracking questions presented the same expectations or intrusion questions as the preceding two but gave response scales that ranged from 0 to 100. These data are reported in the Online Supplement OS.B. Results showed that even giving participants the ability to draw very finely grained distinctions resulted in only minimal variation in expectations as durations increase.

Approximately half the sample, 739 respondents, were asked to rate a series of other law enforcement activities on the same five-point expectations-of-privacy scale used above. Though these results are not central to our project, they provide a sense of how the approach we advocate in the GPS monitoring context would affect the handling of other hot-button Fourth Amendment questions.

Our subjects differentiated sharply among these other types of law enforcement surveillance. On some of these, the public was quite divided. Popular expectations regarding inspection of hotel guest registries, a topic visited by the Court in the 2015 case *City of Los Angeles v Patel*,[195] were exactly evenly split. On tracking a person using cell-site data, on the other hand, about half the participants thought this was a violation of their expectations of privacy, and just under a third

[195] 135 S Ct 2443 (2015).

disagreed. This is a lopsided split, but reasonable people can disagree about whether it is lopsided enough to raise concern.

There were other instances, however, in which a very clear majority of the public either had or lacked expectations of privacy. A supermajority believes that the police's remote activation of the webcam on an individual's personal computer would violate a reasonable expectation of privacy. It is, surprisingly, not well established in the case law whether such tactics amount to Fourth Amendment searches or violations of federal law when engaged in by law enforcement.[196] An overwhelming majority also feels that the police obtaining emails from an internet service provider infringes a reasonable expectation of privacy. Federal law generally requires police to obtain a warrant to access recent email communications,[197] and one circuit court has ruled that the Fourth Amendment also requires the police to get a warrant in order to obtain any emails from an internet service provider.[198] By contrast, most survey respondents were comfortable with police tactics like the installation of a video surveillance camera in a public park where criminal activity had recently occurred. Those who believed such tactics definitely did not or probably did not infringe a reasonable expectation of privacy outnumbered those who had opposite feelings by a 58% to 29% margin (see Table 9). The case law is consistent with popular sentiment here as well.[199]

## IV. Conclusion

This project has both empirical and doctrinal implications. As an empirical matter, we show that very large majorities of the American public do not conceptualize Fourth Amendment expectations

---

[196] See *Clements-Jeffrey v City of Springfield*, 810 F Supp 2d 857, 865–66, 874–77 (SD Ohio 2011).

[197] See, for example, 18 USC § 2703 (Stored Communications Act warrant requirement); 18 USC § 2518 (Wiretap Act super warrant requirement). The government may obtain emails that have been in electronic storage for longer than 180 days via subpoena, provided it gives advance notice to the email user. 18 USC § 2703(b).

[198] See *United States v Warshak*, 631 F3d 266, 288 (6th Cir 2010) (finding a reasonable expectation of privacy in email contents).

[199] See, for example, *United States v Brooks*, 911 F Supp 2d 836, 842–43 (D Ariz 2012). See also *United States v Houston*, 813 F3d 282 (6th Cir 2016) (holding that ten consecutive weeks of video surveillance of a suspect's trailer home and its surroundings via a camera installed on a nearby utility pole did not violate the owner's reasonable expectation of privacy); *United States v Wells*, 739 F3d 511, 522–25 (10th Cir 2014) (holding that someone invited to a guest's hotel room has no reasonable expectation of privacy against video surveillance in the room, and indicating that were the court to hold otherwise the police's ability to conduct such surveillance in public places would be cast into doubt).

Table 9
Results for Other Searches

| | *M* | % Above | % Below | Ratio: Above/Below |
|---|---|---|---|---|
| Remote activate webcam | 4.06 (1.37) | 73 | 15 | 4.74 |
| Obtain emails from ISP | 3.73 (1.40) | 63 | 20 | 3.16 |
| Stingray cell-phone tracking | 3.42 (1.42) | 51 | 25 | 2.03 |
| Cell site data | 3.26 (1.50) | 49 | 31 | 1.57 |
| Inspect hotel guest registry | 2.99 (1.51) | 38 | 38 | 1.00 |
| Facial recognition at Super Bowl | 2.61 (1.54) | 33 | 52 | .63 |
| Camera in public park | 2.40 (1.55) | 29 | 58 | .49 |

NOTE.—Numbers in parentheses are standard deviations. The questions appeared in random order. Participants were asked, Would it violate people's reasonable expectations of privacy if law enforcement:

- Used remote activation software to turn on the webcam on their laptop without their permission?
- Obtained from their internet service provider copies of emails exchanged between them and someone else?
- Used a fake cell tower to trick their phone into giving the police more accurate information about where the phone is?
- Obtained from their cell-phone company stored information about whether their cell phone was near a particular location on a particular day?
- Searched a hotel's guest register to obtain the names, home addresses, and assigned hotel room numbers of the guests who stayed there on a particular night?
- Used facial recognition software to check whether any of the fans entering the Super Bowl stadium match images in a Department of Homeland Security database?
- Installed a video camera to watch a public park where criminal activity has recently occurred?

of privacy in a manner that is congenial to the "mosaic theory." Americans generally regard the police's use of car-based GPS devices to determine an individual's whereabouts as the sort of action that infringes on a reasonable expectation of privacy regardless of whether geolocation information is collected for a long or short period of time. These Americans mostly cite the potential for police abuse and infringements on personal freedom as the basis for their consistently high privacy expectations. A substantial minority of the population regards the use of such devices as unproblematic from a Fourth Amendment perspective and, again, the duration of surveillance does not appear to make much difference. Among members of this subgroup, the much-maligned third-party doctrine finds substantial numbers of adherents. Only a tiny percentage of respondents have differential responses based on the length of surveillance, and even among these respondents the "longer surveillance is more problem-

atic" view is hardly universal. It is fair to say, then, that the people whose expectations of privacy are purportedly at issue when the Court considers the Fourth Amendment's scope are duration-insensitive with regard to geolocation surveillance.

Of course, the Fourth Amendment involves questions of privacy cost as well as expectations, and Americans do believe that longer duration searches are somewhat more intrusive and more likely to expose sensitive information than shorter duration searches. But even there, the salience of duration should not be overestimated. To the extent that courts wish to make surveillance duration relevant, however, the sensitivity/invasiveness calculus is the appropriate doctrinal hook.

Attitudes toward privacy and expectations of privacy are heterogeneous across the population, and this heterogeneity is predictable. Political psychology metrics like Duckitt's Authoritarian Submission Scale correlate with expectations of information privacy in police search contexts. Other demographic variables, like age, plausibly drive the resonance of the third-party doctrine. This article is an early step toward the broader goal of explaining the psychological basis of privacy expectations.

On the doctrinal front, our project offers a cleaner way for courts to resolve Fourth Amendment questions. Fourth Amendment doctrine has become an unpredictable jumble. Instead of a status quo where the courts inexplicably ignore considerations that have been treated as dispositive in previous cases, we offer a straightforward constitutional framework where the same questions are always relevant. First, did the government infringe on a protected property interest? If so, a search has occurred. Second, do Americans generally expect the government to conduct the kind of surveillance it performed in a particular case? If so, then no search has occurred. Third, is the type of search conducted meaningfully likely to reveal sensitive information? If not, then no search has occurred. And, finally, if a warrantless search has happened, do cost-benefit calculations justify permitting that search? Survey data would be irrelevant to the first inquiry, dispositive of the second, relevant to the third, and perhaps informative for the fourth.

We think that the science of survey research has now advanced to the point where analytical clarity is achievable in a manner that takes the idea of "reasonable expectations of privacy" seriously. It is not Justice Alito's fault, nor the fault of other Justices, that their sense of

what people expect is occasionally out of line with what people actually expect[200]—the academy has failed to provide jurists with sufficiently trustworthy data about the public's perceptions. The price of gathering and analyzing survey results from a representative sample of Americans is declining toward zero, and this dropping price-point makes it increasingly feasible for social scientists in the academy to gather such data for the benefit of courts and police departments.

Having covered our empirical and doctrinal contributions, it is worth raising a normative question about whether it matters that the public and the Supreme Court Justices are in this instance out of step in their assessments when it comes to privacy expectations. Does the fact that the mosaic theory fails to resonate with the public's expectations render the theory bad law? We think the failure of duration sensitivity to resonate with the public presents a serious problem. The Fourth Amendment exists for instrumental purposes—it allows people to predict when an action will remain private and when it may become public, and to direct their behavior accordingly. When Fourth Amendment protections and popular expectations are misaligned, people are guarded when they should feel free and feel free when they should be guarded. This creates a real social cost.

One possible reaction to this problem is to conclude that advocates of the mosaic theory have a great deal of marketing and persuasion work ahead of them. If the doctrine is sound as a policy matter, perhaps the solution to our dilemma is to correct the expectations of ordinary Americans. Our other ongoing research makes us inclined to believe that, at least in the short run, such persuasion efforts would be largely futile.

Another possible reaction is to declare that reasonable expectations of privacy for Fourth Amendment purposes have nothing to do with what reasonable Americans expect. We also find this possibility unappealing. The practical costs of disagreement are very real. Absent an anchor to the opinions of ordinary Americans, the content of the Fourth Amendment becomes subject to the whims of unrepresentative legal elites. Given that our data show that basic personality and demographic factors, including age, strongly influence privacy

[200] See note 51; see also *Minnesota v Carter*, 525 US 83, 97 (1998) (Scalia, J, concurring) ("In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those actual subjective expectations of privacy that society is prepared to recognize as reasonable bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.") (citation and internal quotation marks omitted).

expectations, it is inevitable that elite and popular opinion will diverge on these issues. At a time when the Court is famously homogeneous in so many respects,[201] we should not be comfortable if judges and Justices rely entirely on the limits of their personal experiences. Modern social science has developed to the point where the legal system need not and should not tolerate "this is what I think" or "this is what my law clerk thinks" being used as proxies for what members of society generally expect and value. Rather than adopt either of these answers, we have proposed what we think is a more sensible, data-driven approach to the morass that is Fourth Amendment search doctrine. We also note that, unlike in many other areas of law, looking to public expectations here would plausibly result in *increased* constitutional protections. The usual role of courts as protectors of minority rights is actually being inhibited by a failure to consider this evidence.

The mosaic theory emerged from the minds of judges who wanted to guarantee some measure of Fourth Amendment privacy in the digital age without overruling *Knotts*, which held short-term geolocation surveillance to be a nonsearch. We are personally sympathetic to the goals of the mosaic theory. Given how the Fourth Amendment precedents of the 1980s and 1990s interact with the realities of cheap electronic monitoring, some doctrinal innovation is needed to leave space for personal privacy. But we are concerned enough by this disconnect between what the people expect and how judges characterize those popular expectations to become skeptical about whether the revolution in Fourth Amendment jurisprudence that *United States v Jones* seems to foreshadow will prove to be an enduring endeavor. Given these data, rejecting *Knotts* is better than trying to translate the mosaic theory into workable and intuitive doctrine. Returning to the central issue emerging from *Jones*, then, we think it makes sense to stand with the very large group of citizens who label geolocation surveillance of any length an infringement of reasonable privacy expectations rather than with the very tiny group who say that the Fourth Amendment is implicated only if the surveillance lasts long enough.

---

[201] See, for example, Dahlia Lithwick, *The 2014 Supreme Court: An Ivy League Clan*, New Republic (Nov 13, 2014), archived at http://www.newrepublic.com/article/120173/2014-supreme-court-ivy-league-clan-disconnected-reality.

Supreme Court Review
Online Supplement for
*Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*
Matthew B. Kugler and Lior Jacob Strahilevitz

## Overall contents:

This document contains a number of additional analyses that could not be presented in the article text due to space constraints. They are, in order: an entirely new Mechanical Turk study examining the effect of question wording on privacy expectations; a description of the results from the Wave 3 conditions that used 101-point scales; an alternative way of comparing the expectations and intrusiveness data from Wave 3 described in Table 8; and an expanded discussion of the personality factors included in Waves 1 and 2.

## OS.A. Question Wording and the Robustness of Expectations

Any single formulation of a question is inherently limited and subject to criticism. Had we asked whether it violates a person's "privacy" for law enforcement to engage in tracking, we could have been fairly criticized for not asking the right question: is the doctrine not clear that we are concerned with "reasonable expectations" of privacy? But having asked about reasonable expectations of privacy, we can be fairly criticized for asking ordinary Americans to give a legal conclusion rather than a factual impression; how are people to know whether their expectations of privacy are "reasonable?" Rather than engage in a long debate over the best question wording, we decided to test whether wording matters. A study was conducted using a convenience sample of 1144 American adults recruited from Amazon's Mechanical Turk service. This sample was not census-representative.[1] It was, for example, 58.1% male and had a median age of 29. Its baselines therefore should not be taken to represent the views of any definable population or subpopulation. But the purpose of the study was to test whether differences in question wording led to differences in response patterns. Answering this question only requires random assignment to condition, not random sampling of a population.

Six different question variants were tested, comprising a 3 (expectations) x 2 (first or third person) design. The expectations factor varied whether the question asked about "reasonable expectations of privacy," "expectations of privacy," or, simply, "privacy." The first or third person factor varied whether participants were asked if the law enforcement action would violate "your" privacy or whether it would violate "people's" privacy. The questions were otherwise as used in the preceding study.[2] Our prediction was that the expectations manipulation would have no significant effect on

[1] The median age was 29 (range 18–77, M = 32.14, SD = 10.36). 10.8% had graduate degrees, 40.6% had four year college degrees, 19.6% had two year degrees, 28.7% had high school degrees, and .3% had not completed high school. The sample was also substantially less conservative (M = 3.20, SD = 1.53) and less authoritarian (M = 3.03, SD = 1.05) than were the respondents in Waves 1 and 2. The sample originally contained 1205 respondents, but data from 61 were discarded because the participants failed an attention check.

[2] The one exception was a rewording of the locate question. The revised version read "Used a car's onboard GPS system to locate it on public streets at a single moment in time without the owner's permission?" This was different than the version in Waves 1 and 2, which read "Used a car's onboard GPS system to locate it on public streets without the owner's permission?" We believe the revised version is slightly clearer. This study actually included both versions and the results for each did not differ.

participant responses. Based on prior research by Slobogin and Schumacher,[3] however, we expected that participants would report greater privacy expectations for the first person framing than the third person framing. The main question there was whether the first- versus third-person framing would interact with either the expectations manipulation or the search duration effect beyond merely elevating the degree of privacy expectation.

Table S.1: Mean Responses and Variations of Privacy Wording

| | 3rd Person | | 1st Person | | Total | |
|---|---|---|---|---|---|---|
| Privacy | 4.41 | (.89) | 4.61 | (.73) | 4.51 | (.82) |
| Expectation of Privacy | 4.29 | (.98) | 4.50 | (.89) | 4.40 | (.94) |
| Reasonable Expectation of Privacy | 4.23 | (1.11) | 4.48 | (.98) | 4.35 | (1.05) |
| Total | 4.31 | (1.00) | 4.53 | (.87) | 4.42 | (.94) |

A univariate ANOVA conducted on the mean privacy expectation scores (averaging the locate, one day, one week, and one month) responses revealed no significant effect of the expectations factor; it did not matter which version of the question was asked.[4] The first vs. third person factor had the predicted effect, with more privacy violation reported for the first person wording (see Table S.1 for means).[5] There was no interaction between the two manipulations, however, and a mixed ANOVA using the four durations as a within-subjects factor and the two conditions as between-subjects factors revealed only the expected effect of duration.[6] There were no significant interactions between duration and the two experimental manipulations.

The analysis of the means therefore shows only one meaningful effect: privacy (or expectations of privacy, or reasonable expectations of privacy) feels increasingly violated when participants are thinking of searches of themselves than when they are thinking of searches of other people. This effect is not particularly large, but it is statistically significant. There are not, however, any interactions between the experimental manipulations and duration. There is not, for example, any greater difference between one day tracking and one month tracking when participants are thinking of themselves, or when they are answering the expectations version of the question.

Using the consistency categories that we employed for Waves 1 and 2 shows similar results. There are no significant differences across the expectation conditions.[7] There is a significant effect across first versus third person, however, such that there are more people in the consistently high

---

[3] Christopher Slobogin and 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, 749 (1993).

[4] $F(2, 1138) = 2.88$, $p = .06$ $\eta^2 = .005$. This could be seen as a nonsignificant trend, but it is best disregarded given the large sample size (N = 1140) and small effect size. By comparison, the effect size of the duration changes was approximately 20 times as large.

[5] $F(2, 1138) = 15.93$, $p < .001$ $\eta^2 = .014$.

[6] $F(1.74, 1977.26) = 143.51$, $p < .001$ $\eta^2 = .11$. Due to a sphericity violation, the Greenhouse-Geisser correction is reported here. Pairwise comparisons indicated that all durations were significantly different from each other (Locate = 4.19; Day = 4.43, Week = 4.52; Month = 4.55).

[7] Overall $\chi^2(10, 1144) = 12.735$, $p = .24$.

category when the first person wording is used.[8] This is consistent with a general increase in privacy expectations in the first person conditions.

Table S.2: Consistency Categories as a Function of Experimental Conditions

| | Privacy | Expectations | Reasonable Expectations | 3rd Person | 1st Person |
|---|---|---|---|---|---|
| None of these | 4.4% | 8.8% | 9.6% | 9.9% | 5.4% |
| Consistently Low | 3.1% | 4.4% | 5.1% | 4.8% | 3.6% |
| Consistently Middle | 2.1% | 1.6% | 1.3% | 1.9% | 1.4% |
| Consistently High | 62.5% | 56.9% | 58.1% | 52.7% | 65.6% |
| Rising Trend | 24.2% | 23.4% | 21.6% | 25.6% | 20.6% |
| Rising Trend that Crosses | 3.6% | 4.9% | 4.3% | 5.1% | 3.5% |

Overall, then, these data suggest that the choice of a "reasonable expectations of privacy" wording was not decisive in producing the reported results. Had we employed an "expectations of privacy" or merely "privacy" wording we likely would have shown the same pattern. Also, even as radical a change as use of a first person framing only changes the baseline level of responses; it does not interact with the duration levels to suppress or exacerbate duration differences. Our results are therefore relatively robust to wording choices.

Further, we should underscore the vast difference between the baseline responses observed in our Mechanical Turk sample, which skews young and male, and our census-representative sample.[9] Though Mechanical Turk is a convenient mechanism for data collection, these data suggest that it should not be used to establish base rates in on privacy issues; the demographic differences are simply too important.

## OS.B. Number of Points on the Scale.

When we designed Wave 1 of this study, we expected to find support for Justice Alito's view of duration. A median response pattern of locate = 1, one day = 2, one week = 4, and one month = 5 would not have surprised us. That is a large part of why we constructed our scales as we did; we were expecting to show very large movements across questions. Given the pattern we actually observed, however, one could be worried that our use of a five-point scale may have made it easier for our subjects to respond with perfect consistency. Had we used a ten-point or one hundred-point scale, it could be argued, participants may have been more inclined to draw distinctions between short and long searches. To address this concern, we had a portion of the Wave 3 respondents answer the same questions using a 101-point scale.

Recall that the first two versions of Wave 3's question asked about 1.) expectations and 2.) intrusiveness on 5-point scales. The final two versions of the GPS tracking questions presented the same expectations or intrusion questions as the preceding two but gave response scales that ranged from 0 to 100. These scales were presented in the form of sliders that showed a numerical value in the margin, allowing determined participants to choose exact figures. These conditions were included for two reasons. First, Slobogin's work has all been conducted using a 101-point intrusion scale. Using a similar scale for our intrusion measure permits us to see how the level of GPS intrusion we observe compares

[8] Overall $\chi^2(5, 1144) = 22.19$, $p < .001$. A chi square analysis contrasting the prevalence of consistently high responses in each group showed that difference was also significant. $\chi^2(1, 1144) = 19.76$, $p < .001$.

[9] See the discussion in Section III.C. of the article.

to his results for other searches. Second, these slides allow us to test an extreme of question formatting. Our use of 5-point scales to this point was somewhat arbitrary – one could defensibly have chosen to use a 2-point scale (yes, no), a 4-point scale (lacking a midpoint), or an *N*-point scale (allowing finer gradations). A 101-point scale allows participants to draw distinctions as finely as they could wish.

Table S.3: Means for 101-Point Scales

| | Expectations | | Intrusiveness | | Reveal Sensitive Information | | Embarrassment | |
|---|---|---|---|---|---|---|---|---|
| Locate | 60.18 | (35.74) | 61.79 | (32.19) | 59.57 | (31.03) | 55.91 | (33.54) |
| Track 1 Day | 64.85 | (35.33) | 71.35 | (30.41) | 66.29 | (28.84) | 60.47 | (32.96) |
| Track 1 Week | 67.42 | (35.39) | 75.38 | (29.37) | 71.62 | (28.73) | 64.61 | (32.18) |
| Track 1 Month | 69.63 | (35.20) | 79.53 | (28.36) | 76.77 | (26.78) | 68.96 | (31.56) |

There are several takeaways from these results. First, *on expectations* respondents do not sharply differentiate between searches of varying duration even given the ability to draw very finely-grained distinctions. The difference between a locate search and one month of tracking is less than 10 points. Second, on both expectations and intrusiveness, there is virtually no daylight between tracking for one week and tracking for one month. On expectations, a mere 2 points out of 101 separate these two searches. On intrusiveness, a mere 4 points. Statistically, these scores differ.[10] As a practical matter, however, doctrine would need to slide a knife's edge between them in order to treat them as distinct. This presents a challenge for courts attempting to implement the mosaic theory's duration distinction because many of them have attempted to draw a line in precisely this place.

More broadly, the answer patterns are consistent with those generated on five-point scales (compare Table S.3 to Tables 7 and 8 in the article). The expectation differences are extremely tiny, and the intrusiveness differences are slightly larger but still likely not consequential. Also, recall that Justice Alito's concurrence in *Jones* would have held that short-term monitoring was *not* a search whereas long-term monitoring *was* a search. Some of the post-*Jones* case law has similarly drawn this type of binary distinction. It would provide little support for these holdings if participants' expectations were offended "65" by one-day monitoring and "69" by one-month monitoring. Even if that difference were statistically *reliable*, it would not be *meaningful*.

## OS.C. Consistency Categories for Intrusiveness Measures.

Table 8 in the article gave mean scores for the intrusiveness measures on five-point scales, but did not display the results in terms of consistency categories. This data is presented here in Table S.4. As would be expected based on the mean scores, there were consistently more people in one of the rising trend categories for the intrusiveness (31.7%), information (35.6%), and embarrassment (30.4%) measures than for the expectations measure (19.9%).[11]

[10] All differences on all measures are significant at the $p < .01$ level. This is unsurprising given that each cell has over 350 participants and the comparison is within-subjects.

[11] Intrusiveness: $\chi^2(1, 747) = 13.51$, $p < .001$. Information: $\chi^2(1,747) = 22.81$, $p < .001$. Embarrassment: $\chi^2(1, 747) = 10.88$, $p < .001$. Each is being contrasted with expectations.

Table S.4: Consistency Categories for Expectations, Intrusiveness, Information, and Embarrassment

| | Expectations | Intrusiveness | Reveal Sensitive Information | Embarrassment |
|---|---|---|---|---|
| None of these | 16.0% | 16.1% | 19.50% | 19.70% |
| Consistently Low | 15.2% | 8.8% | 6.80% | 10.60% |
| Consistently Middle | 11.0% | 6.5% | 10.60% | 14.30% |
| Consistently High | 37.8% | 36.9% | 27.50% | 24.90% |
| Rising Trend/Not Cross | 13.5% | 22.6% | 23.40% | 24.90% |
| Rising Trend/Cross | 6.4% | 9.1% | 12.20% | 5.50% |

## OS.D. Personality Differences

As we describe in Section III.D. of the article, scholarly understandings of the psychology of privacy are in their infancy and only a few papers have considered whether people with strongly protective privacy views are systematically different than those with comparatively unprotective views. We believe that this is an unfortunate gap. Understanding which personality factors can explain divergences in views of privacy issues enriches our understanding of why judges vote the way they do and how privacy questions may be regarded differently across diverse communities.

Our survey instrument contained several measures that are useful for mapping the effects of personality and political ideology on privacy attitudes. Responses to these measures were analyzed using a between subjects analysis of variance with the response patterns described in Table 2 in the article (with two minor changes) as the between subjects factor.[12] The first change is that the rising trend category was collapsed to include both trends that did and did not cross the midpoint. The second is that the "none of these" response category was omitted as it was likely to contain a highly heterogeneous sample of participants, including some who may have been inattentive. Thus the categories in this analysis are 1.) consistently high, 2.) consistently middle, 3.) consistently low, and 4.) rising trend.

As mentioned in the demographics discussion, the survey included a one-item measure of liberal versus conservative orientation. As can be seen in Table S.5, there were no significant differences on this measure, though an inspection of the means suggests that those consistently low in privacy expectations are very slightly more conservative than others. It therefore does not appear that political orientations are strongly connected to concerns about geolocation tracking.

The survey also contained a measure of authoritarian submission. The social psychological theory of rightwing authoritarianism defines authoritarians as people who are especially willing to submit to authority, who believe that it is particularly important to yield to traditional conventions and norms, and who are hostile and punitive toward those who question authority or who violate such

[12] An ANOVA model compares the mean scores of participants in multiple groups. The overall F statistic shows whether or not the means of groups A, B, and C are statistically distinguishable. If there are differences between the groups, subsequent pairwise tests can show which groups differ from each other.

conventions and norms.[13] The authoritarian submission scale, developed by John Duckitt and colleagues, is intended to measure the first of those impulses: the extent to which people believe that authority should be respected and obeyed rather than challenged and questioned.[14] Items include "It's great that many young people today are prepared to defy authority (reverse coded), and "What our country needs most is discipline, with everyone following our leaders in unity." The response scale ranged from 1 – Strongly Disagree to 6 – Strongly Agree. Higher scores on the authoritarian submission scale indicate stronger endorsement of authoritarian ideologies.

Authoritarianism is one of the two major individual difference constructs in political psychology.[15] It has been shown to correlate with attitudes toward a wide array of political issues including abortion, affirmative action, racial minorities in general, illegal drug use, the homeless, homosexuality, and, among men, hostility toward women.[16] John Duckitt's model of ideological development describes a progression by which people who strongly value social conformity come to see the world as a particularly dangerous place because of the many threats to that conformity.[17] This belief in the dangerousness of the world then prompts authoritarian responses. The general model of perceptions of threat and dangerousness leading to authoritarian-style responses has received substantial support in the psychological literature, though some believe that the mechanism is more nuanced.[18] Past research has also shown that authoritarianism is one of the strongest predictors of attitudes toward both informational and decisional privacy issues.[19] This result may reflect the historical links between privacy protections and autonomy beliefs.[20]

---

[13] See Bob Altemeyer, *The Other "Authoritarian Personality,"* in Mark Zanna, ed, 30 *Advances in Experimental Social Psychology* 47–92 (M. Zanna ed. 1998).

[14] John Duckitt et al, *A Tripartite Approach to Right-Wing Authoritarianism: The Authoritarianism-Conservatism-Traditionalism Model*, 31 Pol Psych 685–715 (2010). The other two authoritarianism scales developed by Duckitt and colleagues (authoritarian aggression and traditionalism) were also administered. Given the overlap between some of the items on those scales and the issues discussed in the survey, however, we believe that authoritarian submission was a better measure of the ideology construct for these purposes.

[15] See generally John Duckitt and Chris G. Sibley, *A Dual Process Motivational Model of Ideological Attitudes and System Justification*, *in Social and Psychological Bases of Ideology and System Justification* 292 (2009); Altemeyer, *The Other "Authoritarian Personality"* at 47 (cited in note 13).

[16] Herbert L. Mirels and Janet B. Dean, *Right-Wing Authoritarianism, Attitude Salience, and Beliefs about Matters of Fact*, 27 Political Psychology 839, 840–41 (2006) (reviewing studies).

[17] See generally John Duckitt et al, *The Psychological Bases of Ideology and Prejudice: Testing A Dual Process Model*, 81 J Personality & Social Psychology 75–93 (2002); Duckitt and Sibley, *A Dual Process Motivational Model of Ideological Attitudes and System Justification* at 292 (cited in note 15).

[18] See David Winter, *Authoritarianism – With or Without Threat?*, 8 International Studies Rev 524 (2006) (reviewing studies); see also Stewart J.H. McCann, *Societal Threat, Authoritarianism, Conservatism, and US State Death Penalty Sentencing (1977–2004)*, 94 J Personality & Social Psychology 913 (2008) (arguing that the directionality of a person's response to threat depends on their innate disposition, though authoritarian responding dominated overall).

[19] See generally Matthew B. Kugler, *Affinities in Privacy Attitudes: A Psychological Approach to Unifying Informational and Decisional Privacy*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2469562 (visited Sept 7, 2015).

[20] Louis Henkin, *Privacy and Autonomy*, 74 Colum L Rev 1410, 1425 (1974)

As expected given the prior research on authoritarianism and privacy, responses to the authoritarianism scale differed significantly across condition. Pairwise comparisons revealed that those with consistently low privacy expectations had significantly higher authoritarianism scores than those in any other category, and those with consistently high privacy expectations had significantly lower authoritarianism scores than those in the rising trend condition. [21] The difference between the consistently high and consistently low groups was moderate, amounting to about half a standard deviation (Cohen's *d* = .43).[22] These results are supported by prior work showing that those high in authoritarianism are consistently less supportive of both information and decision privacy protections.[23] In fact, the same authoritarian submission scale here has previously displayed a moderate correlation with a composite of criminal procedure privacy questions.[24]

The survey also contained a measure of the "Big 5" personality factors. These personality traits – agreeableness, extroversion, conscientiousness, neuroticism, and openness to experience – are generally accepted to be a broad, if not totally comprehensive, measure of personality.[25] A voluminous academic literature in psychology has identified ways in which particular personality traits are more pronounced among people who engage in particular behaviors. For example, people who score highly on extraversion disclose more information about themselves on social networks;[26] and highly conscientiousness respondents are more likely to be politically conservative.[27] More extroverted people are more socially popular and attend more parties; more agreeable and conscientious people are more honest; and people who are more open have more musical inclination.[28]

---

[21] All posthoc tests described as significant are significant at least at the $p < .05$ level.

[22] Cohen's d is a measure of effect size that is used when comparing a difference in group means. Expresses the difference between the group means as a function of the pooled standard deviation scores of each group. In general, a Cohen's d of .2 is considered a small effect, .5 is a moderate effect, and .8 is a large effect, but these classifications are somewhat arbitrary.

[23] See Kugler, *Affinities in Privacy Attitudes* (unpublished) (cited in note 19).

[24] Id. Table 3 of that paper shows a correlation of .37 between the criminal procedure composite and authoritarian submission. Importantly, the previous research in this area concerned privacy *attitudes* rather than privacy *expectations*. This is the distinction between asking people how they would like the world to work and asking them how it actually does work. We suspect this difference in question type explains why the relationship between authoritarianism and privacy attitudes was stronger in the preceding paper.

[25] See generally Paul T. Costa Jr. and Robert R. McCrae, *Revised NEO Personality Inventory (NEO-PI-R) and NEO Five- Factor Inventory (NEO-FFI) Professional Manual* (1992); Oliver P. John and Sanjay Srivastava, *The Big Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives*, in *Handbook of Personality: Theory and Research* 102 (L.A. Pervin & O.P. John eds. 1999); Murray R. Barrick and Michael K. Mount, *The Big Five Personality Dimensions and Job Performance: A Meta-Analysis*, 44 Personnel Psych 1, 1–5 (1991).

[26] Baiyun Chen and Justin Marcus, *Students' Self-Presentation on Facebook: An Examination of Personality and Self-Construal Factors*, 28 Computers in Hum Behav 2091, 2097 (2012); Tracii Ryan and Sophia Xenos, *Who Uses Facebook? An Investigation into the Relationship Between the Big Five, Shyness, Narcissism, Loneliness, and Facebook Usage*, 27 Computers in Hum Behav 1658, 1662 (2011).

[27] Dana R. Carney et al, *The Secret Lives of Liberals and Conservatives: Personality Profiles, Interaction Styles, and the Things They Leave Behind*, 29 Pol Psych 807, 824 (2008).

[28] Sampo V. Paunonen, *Big Five Factors of Personality and Replicated Predictions of Behavior*, 84 J Personality & Soc Psych 411, 415–17 (2003).

The questionnaire battery we administered was specifically designed to be brief.[29] Participants were asked to rate on a scale ranging from 1 – Strongly Disagree to 7 – Strongly Agree whether they saw themselves as, for example, "extraverted, enthusiastic" and "reserved, quiet" (both extroversion).

As can be seen in Table S.5, there were significant differences across subject group on three of the measures: conscientiousness, extroversion, and neuroticism. Though the details of the effects on extraversion and conscientiousness differ, there is a common pattern: those low in privacy expectations are different than all others. Specifically, post-hoc tests revealed that participants in the consistently low privacy expectations group had higher mean levels of extroversion than participants in all other categories. The effect is comparatively small, with the difference between the consistently high and low groups being barely over .2 a standard deviation (Cohen's *d* = .23). Similarly, subjects in the low privacy expectations group also reported significantly higher levels of conscientiousness than those in the other groups. The difference between the low concern group and the middle group was moderate (Cohen's d = .37), but the difference between the low and high groups was fairly small (Cohen's d = .20). Some prior research has also shown a link between extroversion and privacy attitudes.[30] This relationship may suggest that those who have low privacy expectations are more likely to have their views felt in social and political settings; extraverts advertise their views far more than do introverts. Observers may therefore assume that anti-privacy sentiment is more common than it actually is.

[29] See Samuel D. Gosling et al, *A Very Brief Measure of the Big Five Personality Domains*, 37 J Res in Personality 504 (2003).

[30] See Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 Harv L Rev 2010, 2024–27 (2013).

Table S.5: Personality Characteristics as a Function of Privacy Views

| | F (3,1229) | | $\eta^2$ | Consistently High | | Consistently Low | | Consistently Middle | | Rising Trend | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| B5 - Agreeable | 0.34 | | .001 | 5.17 | (1.23) | 5.15 | (1.30) | 5.11 | (1.15) | 5.23 | (1.20) |
| B5 - Neuroticism | 2.62 | * | .006 | $3.00_{ab}$ | (1.36) | $2.87_{b}$ | (1.39) | $3.22_{a}$ | (1.31) | $3.12_{a}$ | (1.43) |
| B5 - Conscientious | 4.62 | ** | .011 | $5.72_{bc}$ | (1.16) | $5.95_{a}$ | (1.09) | $5.52_{c}$ | (1.23) | $5.74_{b}$ | (1.13) |
| B5 - Openness | 2.38 | | .006 | 5.00 | (1.23) | 4.86 | (1.18) | 4.73 | (1.18) | 4.95 | (1.21) |
| B5 - Extroversion | 3.26 | * | .008 | $3.60_{b}$ | (1.47) | $3.93_{a}$ | (1.43) | $3.65_{b}$ | (1.22) | $3.63_{b}$ | (1.50) |
| Liberalism-Conservatism | 1.23 | | .003 | 3.95 | (1.70) | 4.18 | (1.75) | 4.08 | (1.51) | 3.99 | (1.63) |
| Authoritarianism | 11.95 | *** | .028 | $3.50_{c}$ | (1.04) | $3.94_{a}$ | (0.98) | $3.60_{bc}$ | (0.73) | $3.67_{b}$ | (0.92) |
| Educational attainment | 0.64 | | .001 | 3.15 | (1.12) | 3.15 | (1.12) | 3.14 | (1.02) | 3.24 | (1.02) |
| Age | 8.84 | *** | .021 | $47.58_{b}$ | (16.59) | $54.00_{a}$ | (16.21) | $48.97_{b}$ | (16.44) | $49.62_{b}$ | (16.36) |
| Supreme Court Knowledge | 0.87 | | .002 | .51 | (.33) | .53 | (.33) | .48 | (.32) | .52 | (.33) |

*** p < .001; ** p< .01; * p < .05

*Group means are significantly different when they do not share subscripts. So for authoritarianism, the consistently high group (c) is significantly different than the low group (a) but not the middle group (bc*).

Subjects with low privacy expectations reported lower levels of neuroticism than participants in the middle privacy expectations (Cohen's *d* = .26) or rising trend categories (Cohen's *d* = .18), but these were small and there were no significant differences between any groups and the high privacy expectations category.

The survey included a measure of Supreme Court knowledge that consisted of four factual questions about the Supreme Court of varying difficulty. These asked participants to identify the current Chief Justice, report the number of Justices on the Court and the number that are female, and identify which of four Justices voted to uphold the individual mandate portion of the Affordable Care Act.[31] The result was a proportion score ranging from 0 to 1 indicating the percent of questions correct. This measure interestingly did not vary across condition. We had imagined that, given the third party doctrine and the *Jones* decision, either the rising trend or consistently low categories would attract disproportionate numbers of informed participants. But this does not appear to have been the case.

[31] The options for the Chief Justice question were Antonin Scalia, John Roberts, William Rehnquist, and Elena Kagan. The options for the Affordable Care Act question were Clarence Thomas, David Souter, John Roberts, and Anthony Kennedy. The other two questions had fill-in-the-blank style response options. Correct responses to our survey were similar to those of a recent poll by the Pew Research Center, which included some of the same questions but permitted respondents to refuse to answer the questions, which many did. See Meredith Dost, *Dim Public Awareness of Supreme Court as Major Public Rulings Loom*, Pew Research Center (May 14, 2015) archived at http://www.pewresearch.org/fact-tank/2015/05/14/dim-public-awareness-of-supreme-court-as-major-rulings-loom/ (visited July 10, 2015).

Moreover, perhaps surprisingly, neither race nor gender was significantly related to privacy expectations in our survey.

Analyses were also conducted on the demographic measures of age and educational attainment. Though there was no effect of privacy group on educational attainment, those in the low privacy expectations group were significantly older on average than people in the other three groups. This was a moderate effect, with the difference between the consistently high and consistently low group means amounting to 6.42 years (Cohen's *d* = .39). As we note in the article, this finding cuts against the conventional wisdom that younger cohorts do not care about their privacy. At least when it comes to geolocation tracking, younger voters seem more inclined to view surveillance of any duration as contrary to their expectations.

Our surprising finding relating to age has important implications for judicial behavior. Judges tend to be much older than the population at large. Notably, those who endorse the third party doctrine are old (M = 58.45 years old, SD = 15.62) even when compared to the others in the consistently low privacy expectations group (M = 50.57, SD = 16.02).[32] This is a moderate effect (Cohen's *d* = .52), and is coming on top of an already moderate age difference between the low privacy expectations group and the remainder of the sample. The disproportionate appeal of the third-party doctrine to older Americans could help explain its staying power despite its apparent lack of resonance with younger Americans.[33] Interestingly, there was no parallel difference related to the third party doctrine on authoritarianism or Supreme Court knowledge.[34]

[32] $F(1,133) = 7.66$, $p = .006$ $\eta^2 = .054$.

[33] See Section III.D. in the article.

[34] Authoritarianism: $F(1,133) = .10$, $p = .758$. Supreme Court Knowledge: $F(1,133) = 1.41$, $p = .237$.