University of Chicago Law School

Chicago Unbound

Public Law and Legal Theory Working Papers

Working Papers

2015

Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory

Matthew B. Kugler

Lior Strahilevitz

Follow this and additional works at: https://chicagounbound.uchicago.edu/public_law_and_legal_theory

Part of the **Law Commons**

Chicago Unbound includes both works in progress and final versions of articles. Please be aware that a more recent version of this article may be available on Chicago Unbound, SSRN or elsewhere.

Recommended Citation

Matthew Kugler & Lior Strahilevitz, "Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory" (University of Chicago Public Law & Legal Theory Working Paper No. 534, 2015).

This Working Paper is brought to you for free and open access by the Working Papers at Chicago Unbound. It has been accepted for inclusion in Public Law and Legal Theory Working Papers by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.

CHICAGO

COASE-SANDOR INSTITUTE FOR LAW AND ECONOMICS WORKING PAPER NO. 727
(2D SERIES)
PUBLIC LAW AND LEGAL THEORY WORKING PAPER NO. 534

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

SURVEILLANCE DURATION DOESN'T AFFECT PRIVACY EXPECTATIONS: AN EMPIRICAL TEST OF THE MOSAIC THEORY

Matthew B. Kugler and Lior Jacob Strahilevitz

THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

July 2015

This paper can be downloaded without charge at the Institute for Law and Economics Working Paper Series: <http://www.law.uchicago.edu/Lawecon/index.html> and at the Public Law and Legal Theory Working Paper Series: <http://www.law.uchicago.edu/academics/publiclaw/index.html> and The Social Science Research Network Electronic Paper Collection.

**Surveillance Duration Doesn't Affect Privacy Expectations:
An Empirical Test of the Mosaic Theory**
(Forthcoming in the *Supreme Court Review* (2016))

Matthew B. Kugler* & Lior Jacob Strahilevitz**

Abstract:

In the landmark case of *United States v. Jones*, as many as five Supreme Court justices indicated that tracking the geolocation of a car for a month would be a Fourth Amendment search even though tracking the same car for a day would not be. This duration distinction is based on an influential theory of the Fourth Amendment, dubbed the mosaic theory, which posits that the aggregation of several non-searches of the same person might amount to a search. Jurists have justified the mosaic theory's duration-sensitivity by grounding it in their sense of "popular attitudes" regarding privacy expectations. Through an empirical examination of survey responses from three large nationally representative samples totaling over 2800 US citizens, we show that Americans' actual privacy expectations run directly counter to the mosaic theory. Where the mosaic theory says that tracking duration affects citizens' expectations of privacy, ordinary Americans overwhelmingly say it does not. Our data also reveal that younger Americans and those Americans holding the most firmly anti-authoritarian views have significantly greater expectations of privacy in geolocation information than their fellow citizens. Americans do say that longer duration surveillance is more intrusive than shorter duration surveillance, but the magnitude of this effect remains small.

We explore the implications of these findings for the mosaic theory by considering the role of public opinion data in Fourth Amendment doctrine more generally. We ultimately propose a clarified approach to the classic *Katz v. United States* "reasonable expectations of privacy" framework that formalizes the role of public opinion by reframing the first prong of *Katz* to ask whether people in general expect privacy in a given context, and the question of what "society is prepared to recognize as reasonable" in *Katz* as one for which the perceived intrusiveness of a search is germane. To show how survey data could shed light on current Fourth Amendment controversies, we also provide contemporary data about American citizens' privacy expectations when faced with various scenarios. The paper presents new data on popular expectations of privacy with regard to police use of stingray devices, cell tower geolocation, email content analysis, hotel guest registry searches, and various sorts of surveillance cameras.

* Law Clerk to the Honorable Richard Posner, U.S. Court of Appeals, Seventh Circuit, 2015-2016; JD University of Chicago Law School, 2015; PhD in Psychology, Princeton University, 2010.

** Sidley Austin Professor of Law, University of Chicago. The authors thank Paul Crane, Katerina Linos, and Peter Winn for helpful discussions, Adam Chilton, Adam Feibelman, Jancy Hoeftel, Chris Hoofnagle, Orin Kerr, Richard McAdams, Pamela Metzger, Paul Ohm, Eric Posner, Christopher Slobogin, Geoffrey Stone, and Matt Tokson as well as workshop participants at Tulane Law School and the University of Chicago 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.

Table of Contents

I.	Surveillance Duration After <i>Jones</i>	8
II.	The <i>Katz</i> Framework's Ambiguity	12
A.	Are Actual Beliefs Actually Relevant?	13
B.	Four Models of the Fourth Amendment?	16
C.	Surveys as a More Satisfying Methodology	18
D.	How Survey Research Can Restore Coherence to <i>Katz</i> Doctrine.....	28
III.	Empirical Data about Views on Surveillance Duration	31
A.	Participants, Procedure, and Measures for Waves One and Two	32
B.	Main Results.....	33
C.	Explanations	36
D.	Personality Differences	39
E.	Question Wording and the Robustness of Expectations	45
F.	Wave 3: Replication, Intrusiveness, and Suggestive Data on Other Searches.....	47
IV.	Conclusion.....	53

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 Judge Ginsburg of the DC Circuit in the landmark case that ultimately became *United States v. Jones*.

Writing for the appellate court panel, 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 ensembles. 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 bookstore 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.²

This analysis allowed the DC Circuit to reach an otherwise difficult conclusion. A controlling precedent, *United States v. Knotts*, had held that an individual driving a car on public roads has no expectation of privacy in her whereabouts.³ Ginsburg wished to argue that long-term monitoring of an individual is different, 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.⁴

Very soon thereafter, the Supreme Court granted certiorari and agreed to hear the *Jones* case. The majority decided in favor of the defendant on narrow grounds, holding that the installation of the device was a trespass and therefore a search.⁵ To the surprise of many, however, four justices signed a concurrence that evidently doubled-down on Judge Ginsburg's mosaic theory.⁶ Justice Alito, writing for

¹ *United States v. Maynard*, 615 F.3d 544, 558 (D.C. 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.").

² *Id.* at 562.

³ 460 U.S. 276 (1983). 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).

⁴ See David Gray et al., *Fighting Cybercrime After United States v. Jones*, 103 J. CRIM. L. & CRIMINOLOGY 745, 760 (2013).

⁵ *United States v. Jones*, 132 S. Ct. 945, 949 (2012).

⁶ See, e.g., DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 334 (5th ed. 2015) ("Both concurring opinions, involving five justices, embraced 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

Justices 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.⁷

As we will demonstrate below, Justice Alito mostly grounds 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.”⁸ In her separate concurrence, Justice Sotomayor expressed evident approval for mosaic theory-style reasoning, focusing on the conclusions that could be drawn from prolonged surveillance.⁹ She agreed with Justice Alito that “longer term GPS monitoring in investigations of most offenses” would amount to a search, though she did not take an explicit position on whether a search warrant would also be required for short-term geolocation monitoring.¹⁰ Given Alito and Sotomayor's opinions, it seems that there will be five votes for the mosaic theory and its “duration sensitive” approach in whatever case comes next.¹¹

Indeed, post-*Jones* cases indicate that nearly all the justices are beginning to talk about privacy in mosaic theory terms. *Riley v. California* made this particularly clear.¹² The Chief Justice, writing on

Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection.”); *but cf. infra* note 29 (identifying another possible explanation for the duration distinction).

⁷ *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (citation omitted).

⁸ See *infra* section II.A.

⁹ *Id.* 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, e.g., *People v. Weaver*, 12 N.Y.3d 433, 441–442 (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).

¹⁰ *Id.* (“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.”).

¹¹ 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., *supra* note 4, at 764; Kerr, *supra* note 6, at 313; Richard M. Re, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885, 1963 (2014).

¹² 134 S. Ct. 2473 (2014).

behalf of eight justices, held that the police generally could not search an arrestee's cell phone at the time of the arrest without obtaining a warrant. Explaining why the arrestee's wallet could be searched but his cell phone could not, the Court 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.¹³

It is this aggregation of multifaceted information over a long time period – which Roberts viewed as qualitatively distinct from the mere snapshot exposed by prior searches – that so 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.

If fully embraced by the Court, the mosaic theory would upend decades of settled doctrine.¹⁴ 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.¹⁵ 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, actually resonate with the public's 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 the 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 tracking 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

¹³ *Id.* at 2489 (emphasis added).

¹⁴ See Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. 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).

¹⁵ See, e.g., Bedi, *supra* note 14, at 1809; 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 & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Gray et al., *supra* note 4, at 745; Kerr, *supra* note 6, at 311; 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).

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 violated 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.

That duration was of such limited relevance took both of 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 violated a reasonable expectation of privacy. After learning otherwise in wave one of our survey, we supplemented wave two so that respondents who believed that surveillance duration did 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.¹⁶ Notwithstanding the criticism to which this doctrine has been subjected in recent years,¹⁷ about 15% of our sample embraced it and its privacy-skeptical implications. Respondents who felt that both one-day and one-month surveillance *did* violate their reasonable expectations of privacy were far more numerous but slightly less unified in their rationales. The most commonly expressed bases for that view were (1) that the police were likely to abuse any power to obtain the geolocation of an individual's car;¹⁸ and (2) that giving the police such power threatened personal freedom. Both responses commanded majority support among duration-insensitive respondents who felt the surveillance infringed on reasonable expectations of privacy.¹⁹

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

¹⁶ The third party doctrine holds that individuals have no reasonable expectation of privacy that information voluntarily shared with third parties (like the bank, a telecommunications company, or passers by) will not be exposed to the government's agents. *See, e.g., United States v. Miller*, 425 U.S. 435 (1976).

¹⁷ *See, e.g.,* 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 PEPP. 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); *infra* text accompanying note 164. *But see* Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009) (defending the doctrine).

¹⁸ Notably these surveys were conducted in June and July 2014, prior to the prominent controversies surrounding Michael Brown and Eric Garner capturing public attention.

¹⁹ Respondents were asked to select the one or two rationales that best explained their views. Among those with consistently low privacy expectations, 48.9 percent selected one option, 37.8 percent selected two, and the remainder selected three or more. Among those with consistently high expectations, 37.8 percent selected one option, 39.2 percent selected two options, and the remainder selected two or more.

expectation is one that society is prepared to recognize as reasonable.²⁰ More participants drew duration-distinctions in the domain of intrusiveness but, again, consistency was the rule.

Our paper proceeds 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 three divergent approaches to the question of how to treat the suggestion in Justice Alito's concurrence that warrantless surveillance becomes unconstitutional as its duration increases. Some courts have treated Alito's concurrence as something akin to binding precedent, deciding in a Goldilocks fashion whether a particular length of surveillance crossed the constitutional line. Others have ignored or even disparaged Justice Alito's framework, continuing to hold that the duration of geolocation surveillance is irrelevant to the constitutional analysis. Finally, a couple of state supreme courts have deviated from the Alito analysis by holding that geolocation surveillance of any duration amounts to a search under state constitutional law.

Part II offers several arguments about why drawing on reliable social science research regarding 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 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 majority 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 was 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. *Katz* prong 2 would focus on the sensitivity of the information collected by the police, again using survey research results about whether information revealed by particular searches would be sensitive or embarrassing. 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. Several of our secondary findings are also important. First, follow-up questions directed at the duration-insensitive participants showed that concerns about freedom and police abuse largely drive the views of those whose expectations are violated by warrantless surveillance of any duration and the third party doctrine uniquely explains the views of those who regard warrantless long- and short-term geolocation surveillance as consistent with their expectations. Second, our data 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

²⁰ See *infra* text accompanying notes 125-126.

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*

Two cases decided forty-five years apart stand as the most important landmarks of modern Fourth Amendment jurisprudence. In 1967, the United States Supreme Court held that wiretaps are a search under the Fourth Amendment in *Katz v. United States*.²¹ And 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.²² Interestingly, in neither case is the Court's majority opinion the central focus of scholarly inquiry. Rather, it is the primary concurrences – Justice Harlan's in *Katz* and Justice Alito's 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 years, this test was embraced by numerous Supreme Court majorities and has become the key touchstone for determining whether a warrant is generally required before law enforcement can employ a particular surveillance strategy.²³ The framework has taken on importance beyond constitutional law as well. Hence, the *Katz* test also determines whether a defendant's conduct is covered by federal wiretap statutes.²⁴ For nearly 50 years, therefore, courts have spoken of "reasonable expectations of privacy."

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*,"²⁵ and academic commentators

²¹ 389 U.S. 347 (1967); see also CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 13 (2007) ("*Katz v. United States* [is] the most important judicial decision on the scope of the Fourth Amendment.").

²² 132 S. Ct. 945 (2012).

²³ 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).

²⁴ See, e.g., *Huff v. Spaw*, ___ F.3d ___, 2015 WL 4430466 at *3-*4 (6th Cir. July 21, 2015); *United States v. Turner*, 209 F.3d 1198, 1200 (10th Cir. 2000).

²⁵ 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 (D.D.C. 2014).

have referred to it likewise as “*Jones’s* second majority opinion,”²⁶ using Sotomayor’s adoption of portions of Alito’s reasoning as a justification for adding her vote to Alito’s four. Foreseeing the potential importance of Alito’s doctrinal shift, Justice Scalia’s majority opinion made a point of specifically criticizing the salience of surveillance duration in Justice Alito’s four justice concurrence. Scalia wrote:

The concurrence posits that “relatively short-term monitoring of a person’s movements on public streets” is okay, but that “the use of 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.²⁷

After *Jones*, the “vexing problems” raised by Alito’s concurrence have become arguably the most important looming questions in Fourth Amendment law.²⁸ If Justice Alito’s apparent²⁹ nod in the

²⁶ Jonathan Siegel & Kate Hadley, *Jones’s Second Majority Opinion: Justice Alito’s Concurrence and the New Katz Test*, 31 YALE L. & POL’Y 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.”).

²⁷ *Jones*, 132 S. Ct. at 954 (majority opinion). It is perhaps puzzling that Justice Sotomayor signed on to an opinion that contained this language. Yet her separate concurrence indicates that she was joining Justice Scalia’s majority opinion in full. *Id.* at 954 (Sotomayor, J., concurring). A charitable reading of her view is that she is inclined to believe that warrantless geolocation surveillance of any duration is constitutionally problematic, so she agrees with Justice Scalia’s criticism of the Alito framework as underprotective rather than overprotective. Or she may agree with Justice Scalia that it was premature to decide that issue in *Jones*. A less charitable reading is that Justice Sotomayor made a mistake and should have only concurred in the result in *Jones*, as Justice Alito did. Some courts have read Sotomayor’s opinion as agreeing with Justice Alito about *Katz*, see, e.g., *Commonwealth v. Augustine*, 4 N.E.3d 846, 860 n.32 (Mass. 2014) (“Justice Sotomayor, in a separate concurring opinion joined in Justice Alito’s view about privacy.”), which would seem to support the mistake interpretation.

²⁸ 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).

²⁹ 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 shows that the rationale turns out not to be a good prediction of what the public actually expects. See *infra* tbls. 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.

direction of the mosaic theory indeed 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 yet revisited the issue of surveillance duration in the few years since *Jones*, the issue has already arisen in a number of lower court cases. Some courts have treated Alito's concurrence in *Jones* as akin to binding precedent. In *United States v. Skinner*,³⁰ decided about half a year after *Jones*, the Sixth Circuit considered whether tracking a criminal suspect for three days by pinging his phone to determine the closest cell phone towers amounted to a Fourth Amendment search.³¹ 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 as its starting point Justice Alito's opinion, and viewed the difference between 28-day-tracking and 3-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).³²

A subsequent case in Michigan applied *Skinner* and deemed real-time surveillance of several cell phones that lasted between 30 and 45 days to be a search, requiring a warrant supported by probable cause.³³ 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.³⁴ Another subsequent decision, also from a district court in Michigan, went even further than the Court in *Jones* and held that a warrant allowing for cellphone GPS tracking for a 30 day period was invalid for lack of particularity.³⁵ 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."³⁶

³⁰ 690 F.3d 772 (6th Cir. 2012).

³¹ *Id.* at 776.

³² *Id.* at 780 (internal citations omitted).

³³ *United States v. Powell*, 943 F. Supp.2d 759, 774 (E.D. 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.

³⁴ See also *Commonwealth v. Augustine*, 4 N.E.3d 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).

³⁵ See *United States v. White*, 2014 U.S. Dist. LEXIS 166444 (E.D. Mich. November 24, 2014).

³⁶ *Id.* Again, however, the suppression motion was denied under the good-faith exception. See *supra* note 33.

Other lower courts have differed sharply. The court in *United States v. Graham*,³⁷ decided during the same year as *Skinner* and *Jones*, deemed itself not to be bound by the Alito and Sotomayor's concurrences. The *Graham* court read the precedents in this way:

While this Court is cognizant of Justice Alito's statement in *Jones* that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," the law as it now stands simply does not contemplate a situation whereby traditional surveillance becomes a Fourth Amendment "search" only after some specified period of time – discrete acts of law enforcement are either constitutional or they are not. . . . Further, it is entirely unclear what the implications would be of an interpretation of the Fourth Amendment that protects "cumulative data" collected by law enforcement. Taken to its logical extreme, such a reading would theoretically affect entire police investigations, and not just surveillance via cell site location data. . . . If that is how the Fourth Amendment is to be interpreted, then the police could commit a constitutional violation by taking enough individually permissible steps, that in the aggregate, add up to a substantial amount of data being collected on suspect – thereby infringing his reasonable expectation of privacy.³⁸

The *Graham* court can count to five just as well as anyone else,³⁹ but it refused to believe that Justices Alito, Sotomayor, and their three colleagues actually meant the sort of radical doctrinal shift that their opinions indicated. Accordingly, it held that the government's acquisition of two hundred and thirty-five days' worth of historic cell site information without a warrant did not violate the Fourth Amendment.⁴⁰ A recent en banc opinion in the Eleventh Circuit revealed a court deeply fractured over the meaning of the Fourth Amendment after *Jones*, with the majority arguing that the Alito and Sotomayor concurrences changed nothing, the dissenter arguing that the game has permanently changed, and three different concurrences trying to make sense of it all.⁴¹ Indeed, even the district court considering *Jones* itself on remand opined that Justice Alito's proposed distinction between short-term surveillance and long-term surveillance was not the law, though it wound up dodging the question of whether the four-month cell tower tracking information gathered by the police in that investigation was collected unconstitutionally.⁴²

³⁷ 846 F. Supp.2d 384 (D. Md. 2012). The case is presently pending on appeal before the Fourth Circuit.

³⁸ *Id.* at 401-02.

³⁹ *Id.* at 404 n. 15 ("In light of Justice Sotomayor's apparent endorsement of Justice Alito's concurrence, *Jones* can be plausibly understood as having two separate majority opinions. In that case, it appears as though a five-to-four majority of the Court might, in the future, endorse and craft some version of a mosaic Fourth Amendment doctrine.").

⁴⁰ *Id.* at 387 (235 days is the cumulative total from two periods of surveillance.) In *Graham* the government never sought a warrant for the surveillance but it did apply to magistrate judges for orders authorizing the surveillance, pursuant to the Stored Communications Act. *Id.* at 386-87. At issue in *Graham* was whether the Act's provisions fell below the constitutional floor set by *Jones*.

⁴¹ *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc).

⁴² *United States v. Jones*, 908 F. Supp.2d 203, 213-14 (D.D.C. 2012). The district court held the evidence admissible under the good faith exception to the exclusionary rule. *Id.* at 214-16.

The Florida Supreme Court's recent opinion in *Tracey v. State*,⁴³ provides yet another approach to construing *Jones*. *Tracey* reviewed the various concurring opinions in *Jones* and concluded that the duration of monitoring could not be constitutionally decisive, citing *Graham* for this proposition.⁴⁴ Distinguishing away the U.S. Supreme Court's 1983 decision in *Knotts*, the court found that tracking *Tracey*'s cell phones in real time on public roads for one day without a warrant violated the Fourth Amendment.⁴⁵ Surveillance duration was therefore irrelevant because the police action was always a search. Other courts have held that warrantless cell-phone tracking for just one evening is generally unconstitutional under their state constitutions.⁴⁶

With these three 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*, follow the Alito framework and use it to deem warrantless short-term geolocation surveillance constitutionally permissible and warrantless long-term surveillance impermissible.⁴⁷ Other courts, like *Graham*, ignore the duration of geolocation surveillance because they regard the Alito framework as unworkable, holding both long and short-term surveillance permissible.⁴⁸ Finally, other courts may soon follow *Tracey* in rejecting the salience of surveillance duration by holding even very short-term warrantless geolocation tracking impermissible.⁴⁹ As it presently stands, one-day warrantless surveillance is unconstitutional in Florida and New Jersey but 235-day warrantless surveillance is constitutionally permitted in Maryland. That situation cannot represent a stable equilibrium. The Supreme Court will need to revisit the salience of duration in the constitutional analysis soon. In the Part that follows, we will 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" and invokes Fourth Amendment protections depends on whether it violates reasonable expectations of privacy. The most obvious way to

⁴³ 152 So.3d 504 (Fla. Oct. 16, 2014).

⁴⁴ *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.").

⁴⁵ *Id.* at 525-26.

⁴⁶ See, e.g., *State v. Earls*, 70 A.3d 630, 644 (N.J. 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. . . . 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.").

⁴⁷ See *supra* text accompanying notes 30-36.

⁴⁸ *United States v. Wilford*, 961 F. Supp. 2d 740 (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 S.C. 533 (S.C. App. 2015) (following *Graham*, not *Tracey*).

⁴⁹ See *Earls*, 70 A.3d at 630.

determine the privacy expectations of ordinary people is to ask lots of people what level of privacy they expect in a given scenario and tally those responses. Indeed, one might suppose this straightforward approach to resolving questions of what constitutes a search seems so plainly consistent with the text of the *Katz* test that use of a survey methodology would be uncontroversial. As it happens, however, there are fierce disputes among both jurists and scholars as to whether it is appropriate to consult survey data in determining the content of people's reasonable expectations of privacy. The debate is presently unresolved and it continues to preoccupy at least some justices on the Court. In this Part we will highlight some prominent recent judicial statements about Fourth Amendment methodologies, and Justice Alito will again be cast as lead actor. We will then bring into the mix work by Orin Kerr, which shows that courts often resolve *Katz* questions without recourse to reliable data about what ordinary Americans believe and expect in particular contexts. Kerr both describes and defends courts' current practices. We will then present a normative case for integrating survey research into *Katz* doctrine, building on important work previously done by Christopher Slobogin. Along the way we offer both strong and weak versions of the argument. The strong version suggests that survey research should be dispositive on some doctrinal questions concerning reasonable expectations of privacy. The alternative weak and incrementalist version suggests that survey research should be merely informative. Under our strong case approach, the systematic use of survey research data presents a way to resolve a present doctrinal conundrum that has arisen in Fourth Amendment jurisprudence.

A. Are Actual Beliefs Actually Relevant?

Justice Alito is the member of the Court who seems most interested in exploring the relevance of what members of the public actually believe about searches. A recent oral argument exchange highlights his frustration with the present uncertainty over Fourth Amendment methodologies. In October Term 2013, the Supreme 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.⁵⁰ During the oral argument for what would become the Court's landmark opinion in *Riley v. California*, the following exchange occurred between Justice Alito and Judith Mizner, an Assistant Federal Public Defender:

JUSTICE ALITO: In determining whether the examination of information on a cell phone ... constitutes a search, what do you think ... we are doing? Are ... we answering an empirical question, what is the reasonable expectation of privacy of a -- of a person in 2014 who has a cell phone ... on his or her person? Or are we legislating what we think is a good privacy rule?

MS. MIZNER: I think the Court is determining whether or not in 2014 an individual has a reasonable expectation of privacy against government intrusion into a device that carries around an increasingly large percentage of somebody's personal and private information.

JUSTICE ALITO: All right. Well, a lot of that -- part of that is the person must act -- people must actually have that expectation. That must be the expectation of people at large in 2014, that they think that everything that's on their cell phones is private, or they think some of the information on the cell phones is private, or they think nothing on the cell phone is private. Where do you think we should look to answer that question about what people in 2014 think about that question?

MS. MIZNER: I think from the fact that people carry them with them in -- in a pocket or in a purse, that that exhibits an expectation of privacy. You don't expect people to be rummaging through your pockets or -- or through the items you're carrying.

⁵⁰ *Riley v. California*, 134 S. Ct. 2473 (2014).

JUSTICE ALITO: But why is that so? Cell phones are different. I'm not going to ... suggest for a second that there are like things that existed in the pre-digital area. But in the pre-digital era, presumably people didn't have a reasonable expectation of privacy in papers, letters, things like that that they had, of photos in a billfold, numbers, addresses, things that they might -- they might be carrying on their persons. ... So how do we determine what the -- what the new expectation of privacy is now?

MS. MIZNER: I think people did have an expectation of privacy in those items until --

JUSTICE ALITO: Then why was it not a search when ... you searched the pocket of somebody who was arrested and you found the address of someplace?

MS. MIZNER: I believe it is a search, Justice Alito. It's a question of whether it is a search that has been justified by an exception to the warrant requirement ... or the permissible scope of the search incident to arrest. It's still a search.

JUSTICE ALITO: All right. [H]ow do we determine whether ... somebody has a reasonable expectation of privacy in any category of information that is contained on a cell phone?

MS. MIZNER: Because of the interconnectivity of the data, I don't think you can say a person has a reasonable expectation of privacy in this app, but not that app, because you don't know what is linked to any other part of the cell phone. So the rule that provides the security that the Fourth Amendment is intended to give an individual would be to say -- [Justice Sotomayor interrupts and changes the subject.]⁵¹

By our count, Justice Alito asked Mizner the same question -- "On what basis does the Supreme Court conclude that a reasonable expectation of privacy exists?" -- four times. The first time he posed the query, Justice Alito even presented the question as one with two possible answers -- either a descriptive answer (a reasonable expectation of privacy exists because most Americans assume they'd have privacy in a particular context) or a normative answer (a reasonable expectation of privacy exists because the justices think it ought to exist). Yet Mizner never answered Justice Alito's question.⁵²

Justice Alito's implication that the beliefs of actual Americans may provide the most satisfying answer to the "reasonable expectations" conundrum also shows up strongly in his aforementioned *Jones* concurrence. There he described Fourth Amendment reasonable expectations of privacy in a manner that equated them with "popular attitudes," and he warned of the dangers that arise when judges gauge these attitudes by projecting their own beliefs onto those of the public as a whole.⁵³ He referred at various times to reasonable expectations of privacy as "the average person's expectations

⁵¹ *United States v. Wurie* (U.S. April 29, 2014), Oral Argument Transcript, available at 2014 WL 1694920, at *39-*41. *Wurie* and *Riley* were consolidated into the *Riley* opinion.

⁵² 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 U.S. 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.").

⁵³ 132 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* 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)).

about the privacy of his or her movements,”⁵⁴ treated “popular expectations” and “popular attitudes” as synonymous,⁵⁵ and referenced the “circularity” of *Katz*’s reasonable expectation of privacy test, a criticism that only resonates in the context of attitudes actually held by the public.⁵⁶ He differentiated between what the public may prefer and what they may nevertheless believe and expect.⁵⁷ 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 non-search.⁵⁸ To be sure, there is some ambiguity about what methodology Justice Alito’s concurrence was applying;⁵⁹ authors of concurrences can get away with a lack of precision more easily than authors of majority opinions. But on the whole, Justice Alito’s oral argument questioning in *Riley* and the opinion he produced in *Jones* elevated the importance of the average member of the public’s actual beliefs and suggested their centrality to the *Katz* inquiry.

We will defend Justice Alito’s apparent approach to this basic jurisprudential question and show precisely how scientific polling can alleviate concerns that judges will place undue weight on their own beliefs or the beliefs of people in their social orbits. We posit that under *Katz v. United States*,⁶⁰ the Court should recognize subjective expectations of privacy under the Fourth Amendment when it

⁵⁴ *Id.* at 963.

⁵⁵ *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.”).

⁵⁶ *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 the pending case of *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 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*, Oral Argument Transcript (March 3, 2015), at 13, available at http://pub.bna.com/lw/131175US_argued.pdf (emphasis added).

⁵⁷ 132 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.”).

⁵⁸ *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.”).

⁵⁹ 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 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.”) (emphasis added) (citation omitted). Justice Alito does not develop this thought any further, but there is little reason to expect continuity in attitudes between 18th century Americans and 21st century Americans.

⁶⁰ 389 U.S. 347 (1967).

believes as an empirical matter that contemporary, ordinary Americans expect privacy in a particular context.

B. Four Models of the Fourth Amendment?

Recall *Katz*'s two-prong test, with its focus on the suspect's subjective expectation of privacy and the question of whether such an expectation is one that society is prepared to recognize as reasonable.⁶¹ Confusion has abounded in the decades since *Katz* about precisely what Justice Harlan meant when he wrote the test and what the Supreme Court majority that subsequently adopted it took it to mean. The consensus in the scholarship seems to be something like this. *Katz* prong one is nearly always a non-issue 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 new article by Orin Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*.⁶²

Most of the scholarly and judicial discussion of *Katz* has therefore focused on the second prong of the test: whether the privacy expectations are such "that society is prepared to recognize as 'reasonable.'" 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.⁶³ 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."⁶⁴ 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."⁶⁵ If the information can only be indicative of criminal conduct – a dog's detection of cocaine – then gathering it likely is not a search. A third possibility is the "positive law model." Under that approach, the courts are to look to whether the government's conduct would run afoul of some independent legal framework other than the Fourth Amendment.⁶⁶ 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.⁶⁷ Finally, Kerr examines 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

⁶¹ See *supra* text accompanying note 23.

⁶² 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 Knots? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 429 ("[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.").

⁶³ 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.

⁶⁴ *Id.* at 508.

⁶⁵ *Id.* at 512.

⁶⁶ *Id.* at 516-18.

⁶⁷ *Id.* at 517 (citing *Florida v. Riley*, 488 U.S. 445 (1989)).

regulating a particular type of government activity, weigh privacy and security interests, and opt for the better rule.”⁶⁸

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.⁶⁹ Sometimes several models are applied to the same case by the Court, and sometimes the Court makes methodological pronouncements that have a distinct “We have always been at war with Eastasia” quality to them.⁷⁰ But Kerr finds some patterns. For example, the Supreme Court tends to employ the probabilistic model in “group settings,” where the court can consider prevailing social norms that affect interactions among non-governmental actions and the resulting expectations of privacy or publicity.⁷¹ In the colloquy we reproduced a few pages ago, Justice Alito was asking Judith Mizner whether, in Kerr’s terminology, the Court should apply the “probabilistic model” or the “policy model” to decide whether individuals have a reasonable expectation of privacy in the contents of their cell phones.⁷² Kerr argues that this state of affairs, in which the Court picks and chooses which of these four models to apply, is desirable,⁷³ a contention we find unpersuasive because of the risk of doctrinal incoherence and unpredictability.⁷⁴

It is worth emphasizing that Kerr’s helpful framework for analyzing Fourth Amendment expectations predates *Jones*. *Jones* itself seemed to reject, at least provisionally and implicitly, some of Kerr’s arguments. Justice Scalia’s majority opinion removes the “positive law” model from the *Katz* framework, instead requiring that courts decide *before reaching the Katz question* whether law enforcement conduct violated independent rights under applicable state property law.⁷⁵ We might then regard the pre-*Katz* trespass / positive law inquiry as “*Katz* Step Zero.”⁷⁶ 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.⁷⁷ 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

⁶⁸ *Id.* at 519.

⁶⁹ *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).

⁷⁰ GEORGE ORWELL, NINETEEN EIGHT-FOUR (1949).

⁷¹ Kerr, *supra* note 63, at 544.

⁷² See *supra* text accompanying note 51.

⁷³ Kerr, *supra* note 63, at 542.

⁷⁴ It has also been argued that all of these models collapse into an overall assessment of intrusiveness. See, e.g., Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1603 (2010).

⁷⁵ *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’ porch would have been a trespass and thus a search, it was unnecessary for the courts to consider the *Katz* framework. *Id.*

⁷⁶ We coin this phrase in homage to Sunstein’s important article. See Cass R. Sunstein, *Chevron Step Zero*, 92 VA. L. REV. 187 (2006).

⁷⁷ *Jones*, 132 S. Ct. at 959-60 (Alito, J., concurring).

such analysis is the reasonableness inquiry that courts turn to if they decide that particular police conduct constitutes a Fourth Amendment search.⁷⁸ That reasonableness inquiry determines whether a warrant or something less is required before the search can commence.

C. Surveys as a More Satisfying Methodology

In the remainder of this Part we will 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 Justice Scalia 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 populace⁷⁹ generally regards the law enforcement conduct in question as a violation of privacy expectations. With positive law already consigned to a *Katz* Step Zero analysis by Justice Scalia’s opinion in *Jones*, our approach would permit courts to distill *Katz* prong two 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.⁸⁰

We feel that focusing *Katz* prong 1 on an empirical question is not only doctrinally elegant but also normatively desirable.⁸¹ 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.⁸² Or citizens might make inordinate investments in learning the contours of Fourth Amendment law, time and money that could be better spent elsewhere. Disconnects between actual law and perceived law may also provide police officers and prosecutors with undue leverage over

⁷⁸ For a description of the Supreme Court’s turn toward cost-benefit balancing in Fourth Amendment reasonableness doctrine, see SLOBOGIN, *supra* note 21, at 21-47 (developing a proportionality principle of the Fourth Amendment and showing how it is consistent with some of the Supreme Court’s case law); Clancy, *supra* note 69, at 1003-15 (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).

⁷⁹ See *infra* text accompanying notes 139-141 for elaboration on how the populace is to be defined.

⁸⁰ See *infra* text accompanying notes 148-154.

⁸¹ See also *infra* text accompanying notes 117-124 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* 12-17 (unpublished draft, on file with authors); Slobogin, *supra* note 74, at 1602-04, 08.

⁸² 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 and Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 720 (1985).

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” likely isn’t what Justice Harlan had in mind when he penned his *Katz* concurrence,⁸³ there are good reasons why ordinary citizens’ actual beliefs have become more doctrinally salient in the years that followed.⁸⁴

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 decisionmaking, there are other places where incorporating survey results from nationally representative samples could improve judicial decisionmaking. 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. Depending on one’s view of the Constitution, Americans’ normative views about the desirability of requiring a warrant before a search could be conducted might be relevant under *Katz* prong 2 as well.

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 search. These two inquiries are conceptually independent.⁸⁵ 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 potentially 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 in responses, but we should expect

⁸³ See *supra* text accompanying note 23; Kerr, *supra* note 62, at 124.

⁸⁴ 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 *Kyllo v. United States*, 533 U.S. 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 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 B.C. 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 *infra* note 136.

⁸⁵ As a practical matter, there are some connections between expectations and intrusiveness. See *infra* text accompanying note 149.

to find broad consensus around many questions involving law enforcement surveillance.⁸⁶ 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.⁸⁷

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. It may be,⁸⁸ but it is very difficult to collect,⁸⁹ 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.⁹⁰ In fact, there is a large psychological literature showing that sufficiently specific attitude measures are often very good predictors of behavior.⁹¹ A striking new study from the *Proceedings of the National Academy of Sciences* is a particularly good example of this at the group level.⁹² In that study, social scientists took advantage of a feature of Swiss law by which voters actually decided in a referendum whether individual citizenship applicants would be granted Swiss citizenship. Ten years after the actual voting, the researchers presented a nationally representative Swiss sample with profiles of citizenship applicants who had characteristics mirroring those of real

⁸⁶ See generally Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L. J. 727, 737 (1993); Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 82 UNIV. CHICAGO 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 & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity* (in-progress).

⁸⁷ Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1522-23 (2010).

⁸⁸ 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).

⁸⁹ 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.

⁹⁰ 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).

⁹¹ See Icek Ajzen & Martin Fishbein, *Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research*, 84 PSYCH. BULL. 888 (1977); Jason T. Siegel et al., *Attitude-Behavior Consistency, the Principle of Compatibility, and Organ Donation: A Classic Innovation*, 33 HEALTH PSYCH. 1084 (2014).

⁹² Jens Hainmueller et al., *Validating Vignette and Conjoint Survey Experiments Against Real-World Behavior*, 112 PNAS 2395 (2015). Our study asks respondents to make a series of simultaneous pairwise comparisons regarding the duration of surveillance. See *infra* text accompanying note 157 & tbl. 7.

individuals from the earlier referendum.⁹³ When survey respondents were presented with multiple citizenship applicants to choose from, the applicant demographic factors that were outcome determinative in the referendum were also outcome determinative in the subsequent hypothetical survey.⁹⁴ 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.⁹⁵

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, such that expectations will eventually conform with policies that were initially rejected.⁹⁶ To lay our cards on the table, we are unimpressed with the circularity 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. That data, which will form the core of our next paper, indicate that even landmark Fourth Amendment decisions move the needle of Americans' articulated expectations of privacy very little.⁹⁷ A unanimous, well-publicized *Supreme Court* opinion on cell phone 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. Our data indicates 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.⁹⁸ Slobogin has surveyed students⁹⁹ and jury pool respondents¹⁰⁰ to gauge the perceived intrusiveness of

⁹³ *Id.* at 2396.

⁹⁴ *Id.* at 2397-98; *see also id.* at 2400 ("Our main finding is that the stated preference experiments, which simulated the naturalization referendums in the survey, perform remarkably well in capturing the structural effects of attributes that drive voting behavior in actual referendums."). While the survey respondents and voters identified the same demographic factors as most salient in shaping attitudes towards citizenship seekers, there were discrepancies between the absolute vote totals in the survey and the referendum, a gap that might be explained by the ten year temporal gap between the referendum and survey or by other factors affecting external validity. *Id.* at 2399-2400.

⁹⁵ *See infra* text accompanying note 155.

⁹⁶ *Smith v. Maryland*, 442 U.S. 735, 741 n.5 (1979); *see also Jones*, 132 S. Ct. at 962 (Alito, J., concurring) ("The *Katz* reasonable expectation of privacy test . . . involves a degree of circularity."); Kerr, *supra* note 63, at 532 ("[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.").

⁹⁷ *See Kugler & Strahilevitz, supra* note 86.

⁹⁸ *See, e.g., SLOBOGIN, supra* note 21; Slobogin, *supra* note 74, at 1588; Slobogin & Schumacher, *supra* note 86, at 727.

⁹⁹ Slobogin & Schumacher, *supra* note 98, at 737. 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 et al., *The Multiple Dimensions of Privacy: Testing "Lay Expectations of Privacy,"* 11 U. PA. J. CON. L. 331, 344-45 (2009).

¹⁰⁰ SLOBOGIN, *supra* note 21, at 111.

various governmental surveillance techniques. Note a distinction between our research and his on this point; we emphasize expectations of privacy rather than intrusiveness. 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.¹⁰¹ For example, police use of undercover informants does not amount to a search under Fourth Amendment precedents like *Hoffa v. United States*,¹⁰² but Slobogin and Joseph Schumacher found that respondents regard such government investigative techniques as more intrusive than other techniques that the courts have consistently held to be Fourth Amendment searches.¹⁰³

An admitted problem with respect to research by Slobogin and others is that it has not been conducted on a nationally representative sample of Americans.¹⁰⁴ 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.¹⁰⁵ Some of the same scholars followed up in 2014 with a nationally representative study of consumer privacy attitudes.¹⁰⁶ That said, no externally valid recent study delves deeply into Americans' Fourth Amendment attitudes.¹⁰⁷ While Slobogin himself has written about *Jones*, his paper on the subject did

¹⁰¹ Slobogin & Schumacher, *supra* note 98, at 739-42.

¹⁰² 385 U.S. 293 (1966); *see also* *United States v. White*, 401 US 745, 752 (1971) (re-affirming *Hoffa*).

¹⁰³ Slobogin & Schumacher, *supra* note 98, at 740, 738 tbl. 1 (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).

¹⁰⁴ *See* Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951, 964 (2009).

¹⁰⁵ Jennifer M. Urban et al., *Mobile Phones and Privacy* 10 (2012), available at <http://ssrn.com/abstract=2103405> (visited Dec. 8, 2014).

¹⁰⁶ Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261 (2014).

¹⁰⁷ 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 – Katerina Linos & Kimberly Twist, *The Supreme Court, the Media, and Public Opinion: Comparing Experimental and Observational Methods* (2015 unpublished working paper, on file with author). Linos and Twist's sophisticated paper does not examine any Fourth Amendment issues.

Another paper, which post-dates ours by a little while, analyzes the public's normative attitudes about Fourth Amendment issues. *See* Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age* (July 20, 2015 unpublished working paper, on file with author). Though the Scott-Hayward and co-authors paper is well-done in many respects, our research strongly suggests that it suffers from serious external validity problems. 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 infra* note 208 and accompanying text. The size of the discrepancy between our representative sample and Mechanical Turk findings was far larger than we, at least, would have expected, and far larger than we are comfortable with. We therefore believe that one cannot 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

not draw on any new empirical research about public attitudes towards the mosaic theory, so he never posed Justice Alito's "duration sensitivity" question to research subjects.¹⁰⁸ 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 established¹⁰⁹ and 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,¹¹⁰ whether popular attitudes will fluctuate wildly from day to day,¹¹¹ why the content of constitutional provisions should hinge on those attitudes as opposed to doctrines grounded in prior constitutional and property-related precedents,¹¹² and whether popular attitudes about complicated legal and technological issues are meaningful.¹¹³ Slobogin has responded to some of these criticisms,

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 the existence of Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207 (2013). The study was written by a former academic who does not appear to have significant empirical training himself but hired an "instructional design consultant" to help him construct two surveys about cell-phone search attitudes. *Id.* at 212. McAllister's results are reported in an odd way. As best we can tell, the article never tells us who any of his 230 survey respondents for the first survey are, how they were recruited (students? Mechanical Turk? a survey firm? something else?), or whether the sample was representative. *Id.* at 212, 236-47. No demographic information about the respondents is provided. None of his data is reported in a way that comports with general standards of social science. In any event, McAllister's study assumed that respondents would have strong feelings about the differential duration of surveillance, though the way he set up the relevant question there was evidently no real opportunity for respondents to indicate duration insensitivity. *Id.* at 241-42. An earlier study by McAllister has the same methodological deficiencies. See Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475 (2012).

¹⁰⁸ Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, Vanderbilt Public Law & Legal Theory Working Paper No. 12-29 (July 11, 2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2098002. Slobogin's paper is more doctrinal than empirical, and it winds up proposing that surveillance lasting longer than 48 hours generally require a warrant based on probable cause. *Id.* at 24. The 48-hour threshold is not driven by his survey results. Our data shows that this 48-hour distinction is not salient to American citizens. See *infra* Table 3 (showing very little difference in attitudes concerning 1-day surveillance and 1-week surveillance).

¹⁰⁹ Slobogin and Schumacher discuss the external validity of their research at Slobogin & Schumacher, *supra* note 98, at 745-51.

¹¹⁰ Kerr, *supra* note 104, at 965 ("How would judges know when public opinion has changed? And how should courts reconcile dueling surveys?").

¹¹¹ *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.").

¹¹² See, e.g., Solove, *supra* note 87, at 1522; Daniel B. Yeager, *Search, Seizure, and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. LAW & CRIMINOLOGY 249 (1993).

¹¹³ Solove, *supra* note 87, at 1523.

noting, for example that courts routinely interpret survey results in other contexts, like trademark litigation.¹¹⁴ And he points out that replication should alleviate concerns about random sample fluctuations.¹¹⁵ We believe Slobogin acquits himself well in the debate and our studies support many of his points. Notably, our own data on privacy expectations shows nearly perfect stability over a time span of almost a year.¹¹⁶

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,¹¹⁷ mostly taking the *Katz* Court’s invocation of “reasonable expectations of privacy” as the Fourth Amendment lodestar as a given. We do think that the case for placing great weight on survey responses is strongest when lay people 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,¹¹⁸ 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,¹¹⁹ and enhances the risk that the idiosyncratic characteristics of the unrepresentative decision makers will systematically distort their assessments of the social tradeoffs.

Nevertheless, there are alternatives to basing “reasonable expectations of privacy” on what ordinary Americans actually say they 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. Alternatively, the law might focus on how sensitive the information sought by the government is. Finally,

¹¹⁴ Slobogin, *supra* note 74, at 1599-1600.

¹¹⁵ *Id.* at 1599.

¹¹⁶ See Table 9 (comparing the results of wave 3 to those of waves 1 and 2); see also *infra* note 159 (noting that wave 1 and wave 2 of our surveys were statistically indistinguishable on questions concerning *Jones*).

¹¹⁷ See *supra* text accompanying notes 81-84.

¹¹⁸ See, e.g., RICHARD A. POSNER ET AL., *THE BEHAVIOR OF FEDERAL JUDGES: A THEORETICAL AND EMPIRICAL STUDY OF RATIONAL CHOICE* (2013).

¹¹⁹ See, e.g., Dhammika Dharmapala & 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, 183-192 (2007) (describing the implications of the Condorcet Jury Theorem to judicial decisionmaking).

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.¹²⁰

A chief virtue of drawing on popular opinion is that it lends itself to quantifiable results, oftentimes more so than the alternatives. Suppose the Supreme Court is confronted with a new question – does the Fourth Amendment prohibit the NSA’s warrantless collection of metadata concerning email and telephone traffic from tens of millions of Americans?¹²¹ Figuring out whether the NSA’s program satisfies a cost-benefit calculus is close to impossible given the limits of available knowledge. Public opinion data, however, furnishes one highly 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. That sort of data can be obtained at a relatively low cost through the sorts of surveys we describe below.

Nearly all the other data relevant to a rigorous cost-benefit inquiry would be much more difficult to obtain. 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.¹²² Like the person on the street who looks for a lost object under a streetlight, because “that’s where the best light is,” judges may focus unduly on the relatively insignificant “known knowns,” while ignoring the vastly more important “known unknowns.” Worse yet, they may use unreliable guesswork or their ideological priors to assess the importance of the known unknowns. The notion that the results generated by such an inquiry will be reliable and predictable *ex ante* is hard to defend.¹²³ By contrast, conducting a poll to assess popular attitudes about NSA

¹²⁰ See *supra* text accompanying notes 63-68. Of course, the courts could substitute a deontological framework for a consequentialist one in assessing the propriety of government surveillance. See Sklansky, *supra* note 14, at 1110-15.

¹²¹ See *generally* *Klayman v. Obama*, 957 F. Supp.2d 1 (D.D.C. 2013) (holding that parts of the NSA program are searches); *Smith v. Obama* (9th Cir.) (argued Dec. 8, 2014) (still pending on appeal).

¹²² The cost-benefit calculus may be more manageable when used to evaluate more routine and familiar law enforcement strategies like stop-and-frisks or roadblocks, though we should not kid ourselves about the ease of evaluating such policies empirically. None of this is to suggest that there is no role for welfarism in the law. Rather, the suggestion is that when technologies and law enforcement strategies whose effects are uncertain are at issue, the results of welfarist analysis will be unpredictable and unreliable. Survey research, which is relatively objective, and which may both inform and be influenced by welfarist considerations, is plausibly a more appealing place to look when evaluating the law enforcement strategy’s legality.

¹²³ Although the NSA example we reference above is one where precise balancing is exceedingly difficult, we are inclined to think that analytical difficulty is more the rule than the exception. Consider the Supreme Court’s most recent Fourth Amendment controversies – Must the police get a warrant before searching a cell phone incident to its owners’ arrest? Must the police get a warrant before searching a hotel’s guest registry? Should the police need a warrant to search the curtilage of a private residence with a drug sniffing dog? It is perhaps not unduly

Surveillance and the Fourth Amendment is cheap and quick, at least for people with the pertinent technical training.¹²⁴ Social scientists employing divergent methodologies are going to obtain broadly consistent results provided they use state of the art techniques for assessing popular sentiment.

A final point about the policy model is worth underscoring. 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.¹²⁵ 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.¹²⁶ Considering the utilitarian calculus with respect to both the scope of the Fourth Amendment and the question of whether dispensing with the warrant requirement, probable cause, reasonable suspicion, or some other safeguard is appropriate double counts utilitarian interests, potentially slanting the doctrine against finding violations of the Constitution.¹²⁷

Now suppose that in light of all the problems with collecting accurate data that informs Kerr's "policy model" of decisionmaking, a court pivots to the "private facts" model, where the sensitivity of the information the government collects (or intends to collect) determines the likelihood of the collection amounting to a Fourth Amendment "search." Resolving questions about sensitivity without the benefit of survey research has some of the same problems as the policy model, though they are less pronounced. 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.¹²⁸ People and even cultures are heterogeneous with respect to what information about themselves they are willing to share, with whom they are willing to share it, and under what circumstances sharing is appropriate.¹²⁹ Differences in

burdensome to assess costs and benefits in a back-of-the-envelope way, but to develop an answer that satisfies rigorous cost-benefit analysis would entail running randomized controlled experiments, assessing difficult-to-measure chilled economic activity, conducting willingness-to-pay surveys, conducting observational studies of gang behavior, and then assessing how a change in a legal rule would affect these measures. The error bars around courts' initial assessments are going to be very high.

¹²⁴ The out of pocket cost for our large-sample survey was \$4550. Obviously, this figure does not include the authors' imputed wages for designing the survey and analyzing the results.

¹²⁵ See, e.g., *Grady v. North Carolina*, 135 S. Ct. 1368, 1371 (2015).

¹²⁶ See *supra* note 78.

¹²⁷ 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.

¹²⁸ See, e.g., HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2009); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. ____ (forthcoming 2015), available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501002>.

¹²⁹ James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004); Adam M. Samaha & Lior Jacob Strahilevitz, *Don't Ask, Must Tell, and Other Combinations*, 103 CAL. L. REV. ____ (forthcoming 2015), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551074.

individuals' psychological worldviews contribute to this heterogeneity,¹³⁰ and the result is that it can be difficult to determine what counts as sensitive. Also, information that was not sensitive when collected may become more sensitive over time. Data that individuals purchase lotions and multivitamins at a department store likewise seems unobjectionable, but the banal becomes highly sensitive when data mining shows that many women who start making certain purchases suddenly are quite likely to be in the early stages of pregnancy.¹³¹ Similarly, municipal data sets showing taxi drivers' trip patterns seem innocuous enough until a data miner discovers that Muslim drivers can be identified because they are invariably inactive during the daily calls to prayer.¹³² That said, the "private facts" model may permit the state to develop workable rules of thumb for both the police and citizenry. Police usually know what kind of information they are seeking and are likely to encounter. In that sense, it is a more workable alternative to the policy approach.

Yet this again leads us to public opinion data. The best way to address the question of sensitivity in an objective and replicable way is to poll a representative sample of ordinary Americans and see what they say is sensitive. 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.¹³³ Taking a shortcut by substituting judicial hunches for the actual view of the populace seems 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 example¹³⁴), but in these easy cases survey respondents will get the answer right too.¹³⁵

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,¹³⁶ and if even that is too pricey our own aim is to collect lots of this data over time and make it freely available on the Internet. We provide some of that data in

¹³⁰ 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>.

¹³¹ Charles Duhigg, *What Does Your Credit-Card Issuer Know About You?*, N.Y. TIMES, May 12, 2009, at MM40.

¹³² Anna Berlee, *Using NYC Taxi Data to Identify Muslim Taxi Drivers*, THE III.ORG BLOG, Jan. 21, 2015, at <http://theiii.org/index.php/997/using-nyc-taxi-data-to-identify-muslim-taxi-drivers/>.

¹³³ See, e.g., SLOBOGIN, *supra* note 21, at 110-13, 183-84.

¹³⁴ See, e.g., *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993).

¹³⁵ See, e.g., Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* at 7, Nov. 12, 2014, available 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).

¹³⁶ The authors would like to conduct surveys like the ones we describe in this paper 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 *supra* note 107.

Table 13. Evaluating the likelihood that information the government collects will be regarded as sensitive down the road is more difficult. Assessing ex ante whether a court is likely to view warrantless surveillance as satisfying a cost-benefit test is harder still, especially when a new program is under consideration. If courts were to deem survey data legally salient, they would be imposing manageable burdens on law enforcement.

D. How Survey Research Can Restore Coherence to *Katz* Doctrine

This brings us to our final point before we dive into the data. Recall the place we started. 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, a development that Orin Kerr attributes to 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.¹³⁷ But what if there is a better way to be faithful to both *Smith* and the version of *Katz* that emerged from *Jones*?

Combining *Smith v. Maryland* with *Jones* one could instead apply the *Katz* test in three steps. Beginning with *Katz* Step Zero, through the lens of *Jones*, one would ask whether the police's 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 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 the defendant expected privacy in a particular situation. Because getting inside the defendant's head is hard, 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 in a particular situation,¹³⁸ 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.¹³⁹ Indeed, in our view, if most members of a discrete and insular minority would expect privacy in a particular setting, then *Katz* prong 1 should be satisfied regardless of whether a particular defendant

¹³⁷ See Kerr, *supra* note 62, at 128-33.

¹³⁸ It is perhaps puzzling why the law should care inherently about the individual defendant's actual expectation of privacy. If the defendant understood that he was exposing incriminating information to public scrutiny, but did so anyway and got caught, then the subjective portion of the test would seem to punish relatively astute criminals and protect relatively clueless ones. See Cloud, *supra* note 78, at 250. It might also benefit risk averse defendants and disadvantage risk seekers. It is hard to think of a good justification for these effects. Perhaps theories of consent explain the subjective inquiry. Information starts out with the individual and we want the law to respect personal choices to keep it private or expose it to the public. But given that courts articulate precedents that guide thousands of people who will never litigate, a long digression in a published opinion about whether a particular individual actually expected privacy seems less helpful than a generally applicable inquiry into whether most people actually would have expected privacy in a (recurring) circumstances. From an ex ante perspective, improving the alignment between the law and expected outcomes reduces the transaction costs associated with learning the law and modifying one's behavior by taking excessive or inadequate precautions. See *supra* text accompanying note 82-83.

¹³⁹ In the trademark context, even confusion among 15 percent of the relevant population is considered substantial. See, e.g., Daniel Gervais & Julie M. Katsko, *Who Cares About the 85 Percent? Reconsidering Survey Evidence of Online Confusion in Trademark Cases*, 96 J. PAT. & TRADEMARK OFF. SOC'Y 265 (2014).

happens to be a member of that discrete and insular minority. In our data set, neither race nor gender has any measurable association with privacy expectations towards GPS tracking. But we can imagine situations in which race or gender could influence peoples' expectations, and in those instances we want to make sure that the law protects potentially marginalized subgroup members.¹⁴⁰ To do that in a manner consistent with the Fourteenth Amendment, Fourth Amendment doctrine likely needs to protect everyone.¹⁴¹

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 prong of *Katz* now gives the courts an opportunity to consider the “private facts” model, either alone or in conjunction with the “policy” model. Here too, public opinion data may be relevant. Courts must have a sense of what information is considered “private” to assess whether a particular technique implicates sensitive “private facts.” If the *Jones* majority's efforts to move property law to a pre-*Katz* inquiry prove unsuccessful, courts would also integrate their analysis of existing property law protections into *Katz*'s second prong.

We think this approach is basically what the Supreme Court was trying to do in *Smith v. Maryland*, 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. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. . . . Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making

¹⁴⁰ A good example is *Safford Unified School District # 1 v. Redding*, 557 U.S. 364 (2009), a case involving a school's search of a thirteen-year-old girl's undergarments. Justice Ginsburg 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*, N.Y. TIMES, July 7, 2009, at MM22. (“Q: What about the case this term involving the strip search, in school, of 13-year-old Savana Redding? Justice Souter's majority opinion, finding that the strip search was unconstitutional, is very different from what I expected after oral argument, when some of the men on the court didn't seem to see the seriousness here. Is that an example of a case when having a woman as part of the conversation was important? JUSTICE GINSBURG: I think it makes people stop and think, Maybe a 13-year-old girl is different from a 13-year-old boy in terms of how humiliating it is to be seen undressed. I think many of [the male justices] first thought of their own reaction. It came out in various questions. You change your clothes in the gym, what's the big deal?”).

¹⁴¹ Under our framework 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. That is why we focus on discrete and insular minorities here.

annoying or obscene calls. . . . 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.¹⁴²

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. 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 1970’s and some of its factual inferences seem to assume a higher level of sophistication than ordinary Americans typically possess.¹⁴³

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.¹⁴⁴ The Court rejected this argument too, 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.”¹⁴⁵ With this sentence, the Court indicated that it hardly cared what Smith himself thought.¹⁴⁶ 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.¹⁴⁷

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 some courts seem to be doing,¹⁴⁸ we would propose resuscitating it by making popular expectations central to the inquiry of 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 comes increased predictability. Under our approach, popular sentiment gauged by reliable social science methods would become a necessary (though not

¹⁴² *Smith v. Maryland*, 442 U.S. 735, 742-43 (1979).

¹⁴³ See *Smith*, 442 U.S. at 748-49 & n.1 (Marshall, J., 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.

¹⁴⁴ *Id.* at 743.

¹⁴⁵ *Id.*

¹⁴⁶ See also *supra* note 138.

¹⁴⁷ *Id.*

¹⁴⁸ See Kerr, *supra* note 62, at 131.

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 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.¹⁴⁹ Second, though both our approach and Slobogin's approach are driven by survey data, we use that 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.¹⁵⁰ His surveys invite normative judgments on the part of laypeople, and some subsequent researchers have done likewise.¹⁵¹ We, by contrast, are primarily asking for descriptive assessment by laypeople – how unexpected would this be? – and then are using our responses to slide 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 that data to a divergent doctrinal use. That said, we think a data-driven approach to determining sensitivity – along the lines suggested by Slobogin – would be worthwhile. 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.F.

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 open 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?

III. Empirical Data about Views on Surveillance Duration

So far we have shown that the lower courts are divided about how to deal with Justice Alito's suggestion in *Jones* that the duration of geolocation surveillance will be a decisive consideration in determining whether it is a search. We have also shown the potential utility of using public opinion surveys to help resolve the duration-salience question and, for that matter, other Fourth Amendment questions about what constitutes a search. Our discussion suggests that hard data about Americans' expressed beliefs is, at a minimum, highly relevant to the constitutional inquiry. At best, the data could be dispositive in many cases.

But this raises an obvious problem. What if the American people are as divided as the courts are over the question of duration salience? If there is no clear consensus about the importance of geolocation-tracking surveillance, then a resort to survey research will achieve little good. Happily, it

¹⁴⁹ Compare *Jones*, 132 S. Ct. at 962-63 (Alito, J., concurring), with *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring).

¹⁵⁰ SLOBOGIN, *supra* note 21, at 180-96.

¹⁵¹ See Scott-Hayward et al., *supra* note 107, at 39-40.

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.¹⁵²

A. Participants, Procedure, and Measures for Waves One and Two

A weighted sample of adult Americans was recruited by Toluna, a professional survey firm with an established panel.¹⁵³ The sample was drawn to mirror closely the American population as a whole across various demographic dimensions. 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 our data analysis.¹⁵⁴ The final sample contained 1461 participants, all of whom were adult US Citizens.¹⁵⁵ The median age was 51 (range 18-95, M = 48.56, SD = 16.80). 51.3% of the sample was female. Slightly more of the sample than the national population as a whole had completed at least some college coursework, but otherwise the educational attainment of the sample was roughly equivalent to that of the broader population.¹⁵⁶ 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. When asked to rate their political orientation 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. Participants were also assessed on a variety of dimensions including the Big 5 of personality, authoritarian submission, media consumption habits, and their knowledge about the Supreme Court.

¹⁵² See *infra* note 161.

¹⁵³ For discussion of demographically weighted panels and online-versus-telephone surveys, see generally J. Michael Brick, *The Future of Survey Sampling*, 75 PUBLIC OPINION Q. 872, 881-85 (2011); Dan Farrell & 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).

¹⁵⁴ Wave one data were gathered June 11-12, 2014. Wave two 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.

¹⁵⁵ 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.

¹⁵⁶ 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 US 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*, online at <http://www.census.gov/hhes/socdemo/education/data/cps/2012/tables.html>.

For the key question, participants were asked whether it would “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 non-trespass cases that have arisen in the wake of *Jones*.¹⁵⁷

B. Main Results

Most obviously, the participants were more likely than not to believe that this type of GPS tracking represented a violation of 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.¹⁵⁸ 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 discernable effect of tracking duration.¹⁵⁹ People were more 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, more by day-long than instantaneous.¹⁶⁰

¹⁵⁷ See notes 30 – 40 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 and we did not want media coverage of the opinion to influence responses to our question.

¹⁵⁸ One-sample *t* tests revealed that all mean scores were significantly above the scale’s midpoint value of 3. *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 the $p < .001$ level.

¹⁵⁹ A mixed analysis of variance was conducted to examine whether there were consistent differences between participants’ responses to the four GPS tracking questions. As mentioned above, there were no effects of wave and no interaction between wave and item. Wave: $F(1, 1459) = .82, p = .37$; interaction $F(1.98, 2884.80) = .16, p = .85$. This means that there were no differences on any of the items across waves and that the pattern of responses across items (whether tracking for one duration was different than for another) did not vary in each wave

The within-subjects portion of this type of mixed analysis of variance assume that the difference score created when comparing condition A to B has the same variance as that created by comparing B to C, and so on. When that assumption of sphericity is violated, the commonly accepted solution is to use a Greenhouse-Geisser correction to adjust the degrees of freedom for the within-subjects portions of the analysis. Here, a sphericity violation was found using Mauchly’s test and the Greenhouse-Geisser correction was employed.

¹⁶⁰ $F(1.98, 2884.80) = 33.62, p < .001, \eta^2 = .023$. All pairwise comparisons are significant at the $p < .05$ level.

Table 1: Effect of Duration on Privacy Expectation.

	Mean	Std. Deviation	Percent below midpoint	Percent 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%

Reponses were on a 1 -5 scale with higher values corresponding with greater invasion of privacy. All pairwise comparisons are significant.

This effect of duration on expectations hides an underlying consistency in responses across measure, however. 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 forty percent of respondents consistently reported that people’s expectations of privacy would be violated for all searches (giving ratings of all fours or all fives).¹⁶¹ A further 16.9% consistently reported that they believed expectations of privacy were not violated (all 1s or all 2s), and 11% consistently gave the middle response (all 3s). 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. While Justice Alito’s duration-sensitive approach received a warm reception from at least three of his Supreme Court colleagues, a national sample reveals that nearly nobody else thinks about geolocation surveillance in the way that he does.

Table 2: Patterns of Privacy Responses.

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%

Proportion of participants using each of the above response patterns.

The “none of these patterns” category represents a puzzle: why would anyone not report equal or greater privacy invasions as the duration of monitoring increased? A portion of the respondents in that category appeared to be particularly sensitive to the use of a GPS device to determine where a vehicle is *right now*, reporting a high level of privacy invasion for that item and lower scores for longer duration monitoring. Others may have made erroneous assumptions about the level of precision employed in the tracking – perhaps believing that long-term tracking would be necessarily less granular

¹⁶¹ Fully 45.4% of respondents gave only 4s or 5s (in some combination) on this question, versus 19% who gave only 1s or 2s. This is a 2.39:1 ratio.

than short-term tracking. Perhaps some of these respondents found our questioning confusing in other respects or did not read the questions carefully enough. As the study was not designed to test and differentiate between these (comparatively rare) perspectives, we cannot make any definitive statement about what was driving these responses.

We expected to find support for the Alito view when we designed this study. A median response pattern of 1, 2, 4, 5 would not have surprised us. That is a large part of why we designed 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. As a purely methodological matter, this is correct. Participants are, in general, more likely to draw finely-grained distinctions if they are given finely-grained scales. But two points mitigate this concern. First, participants did have two options above the midpoint and two options below it. Even if they felt their privacy expectations were violated in every case, they could have responded 4, 4, 5, 5 to express that they were more violated by longer searches. Conversely they could have responded 1, 2, 2, 2 if they felt their expectations were never violated but that they were growing increasingly uneasy as the search lengthened. Despite these opportunities, two-thirds of participants gave perfectly consistent responses to all four questions rather than draw any distinctions. Second, 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.¹⁶² It would provide little support for these holdings if participants' expectations were offended "90" by one-day monitoring and "95" by one-month monitoring. Even if that difference were statistically *reliable*, it would not be *meaningful*; the monitoring would be a search for Fourth Amendment purposes at both durations. We address this point further in a follow-up study reported in Table 12.

Looking question by question, the level of consistency appears to be even higher than it did at the categorical level. Recall that Table 2 requires *perfect* consistency across all four questions in the first three categories. A person who responded 4, 5, 5, 5 would be counted in the "rising trend that does not cross the midpoint category" rather than the "consistently high" category, for instance. Table 3 reports the percentage of people giving the same response to each question from every possible question pair. Obviously there is more consistency between neighboring questions – locate is closer to one day than to one week and one week is closer to one month than it is to locate – but the general theme is one of extreme consistency. The lowest level of consistency between questions is 71.6% and the average is 79.6%. In contrast, the average level of consistency among questions using the same response scale to assess privacy expectations in other contexts was 41.9%, with the lowest pair having 24.9% consistency.¹⁶³ So, though there are plainly people who consistently have high expectations of privacy and consistently have low expectations of privacy, there is a surprisingly high degree of consistency on these particular questions about surveillance duration. One could easily have, consistent with the mosaic theory, predicted that the aggregation of search days represented by month-long tracking would

¹⁶² See *supra* text accompanying notes 22-49.

¹⁶³ Five questions using the same reasonable expectation of privacy response scale were asked on topics such as use of facial recognition technology at sporting events and obtaining emails from an internet service provider. These questions immediately preceded the *Jones* items and also included the attention check, described in note 155.

be viewed as substantially distinct from the quantum of searching represented by a day. Despite the vastly different levels of information that are revealed by prolonged and brief tracking, however, they are largely viewed as the same type of search. 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.

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%

C. Explanations

After the Wave 1 data were collected and analyzed, it became clear to us that there would be a meaningful number of consistently high and low respondents in the second wave. Respondents in Wave 2 who reported consistently low or consistently high privacy expectations were therefore asked to report their reasoning on a subsequent page. Immediately after giving their privacy ratings, these participants were directed to a page that noted they 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 those 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. The third party doctrine has been routinely attacked for, among other reasons, not being consistent with everyday understanding of privacy.¹⁶⁴ It is therefore particularly interesting to see that most of those who express low privacy concern actually do cite it as a driving force in their analysis.¹⁶⁵

¹⁶⁴ See, e.g., Slobogin & Schumacher, *supra* note 86, at 734, 740; Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 HARV. J. L. & TECH. 199, 214-15 (2011); see also *supra* sources cited note 17.

¹⁶⁵ Other data we collected supports the robustness of third-party doctrine beliefs among this subgroup. Majorities of the respondents who found the third-party doctrine compelling in the OnStar example also expressed expectations that were consistent with the doctrine when confronted with vignettes where it applied. In data that we collected as part of this same survey for the purposes of collecting the data in Table 13, we found that those who used the third-party doctrine to explain their consistently low expectations of privacy also had low expectations in settings where email communications had been shared with Internet Service Providers, facial recognition software was employed in public places, surveillance cameras were used in public parks, and historic cell site information was obtained from mobile phone providers. By contrast, this group of respondents had high expectations of privacy in a vignette involving the remote activation of a webcam, when the third party doctrine would be inapplicable. In the webcam example, 50% of third-party-doctrine adherents viewed the surveillance as definitely a violation of reasonable expectations of privacy and 11.4% viewed it as a probable expectation of privacy. (For all other respondents those rates were 60.8% and 12%, respectively). In every other instance, where the third party doctrine does apply, a majority of third party adherents viewed the surveillance as not infringing a reasonable expectation of privacy. The relevant figures were as follows: Facial recognition (3rd party group – 63.6% say not an infringement versus 48.5% of everyone else); Camera in park (3rd party – 69.3% versus 52.6%);

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. Other plausible theories – such as the danger inherent in driving justify the privacy invasion – did not attract high levels of support.

Table 4: Reasons Given by those with Consistently Low Privacy Expectations
(16.9% of the sample)

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%

*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.*¹⁶⁶

Two concerns predominated among those who consistently exhibited high privacy expectations: that the police would abuse GPS tracking if they were free to use it and that even locating a car through GPS tracking imposes substantial restrictions on personal freedom. 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 process 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 reveal a meaningful amount of personal information.¹⁶⁷ According to this theory, the potential for

Stingray device (3rd party – 55.7% versus 30.7%); Emails (3rd party 51.1% versus 29.6%); Historic cell site (68.2% versus 38.8%). Note that the “everybody else” category includes those who consistently did not expect privacy in the GPS On-Star scenario but for reasons besides the third-party doctrine.

Refined versions of these webcam, cell site, facial recognition, etc. questions were included in wave III of the survey and those results are reported in Part III.F.

¹⁶⁶ 41% of respondents selected one explanation, 39% selected two, and 20% selected more than two.

¹⁶⁷ *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)

government observation of one's location can create a substantial chilling effect on innocuous, or even beneficial, behaviors. Though only a fairly small minority (21%) endorsed the argument that even a short monitoring period could reveal as much about a person as would a long period, the endorsement of the other item suggests that even the amount of information revealed by short term monitoring disturbed many participants.

Roughly a third of participants who consistently found an expectation of privacy endorsed a property-based view. These participants objected, at least in part, because the car's own GPS system was used to track the vehicle. This explanation comes closest to that endorsed by the *Jones* majority opinion. Recall that there the Court held that GPS tracking constituted a search because the police installed their own GPS device on the suspect's car, thus invading the suspect's property under *Katz* step zero.¹⁶⁸

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

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%

Numbers display the percentage of participants selecting each of the available options. Participants were encouraged to select the best one or two options, but were not limited to that.

It is also interesting to consider the explanations for both outcomes that few participants endorsed. One theory rejected by those who regarded surveillance of any duration as problematic 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 longstanding resource constraints on government investigations continue to inform reasonable expectations of privacy,¹⁶⁹ Justice Alito's

¹⁶⁸ See *supra* text accompanying note 22.

¹⁶⁹ *Jones*, 132 S. Ct. 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 . . .’”).

discussion of the “very tiny constable” needed for 18th century carriage tracking,¹⁷⁰ and Orin Kerr’s equilibrium adjustment model.¹⁷¹ There is something intuitively 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.

Also, the idea that monitoring on public roads is always okay only attracted a third of the privacy-unconcerned participants. This type of reasoning, suggestively endorsed by the Supreme Court in *Karo*,¹⁷² played a distinct second fiddle to the unexpected popularity of the third party doctrine. It should be remembered, however, that the third party doctrine was only popular among those who never felt surveillance of any duration violated a reasonable expectation of privacy. Overall, that doctrine was endorsed by 11.6% of the sample. In contrast, 39.5% of the sample consistently rated a GPS search as a definite violation of reasonable expectations of privacy.

Finally, the various forms of privacy absolutism attracted fairly little support. Few respondents were willing to state that privacy was simply an obsolete concept, or that security interests should always trump privacy interests. Similarly, not many of the respondents who rated tracking of any duration as problematic stated that privacy should always trump security.

D. Personality Differences

We approach the issue of Fourth Amendment law with a particular interest in the psychological underpinnings of privacy sentiment.¹⁷³ Scholarly understandings of the psychology of privacy are in their infancy, and the legal literature on the use of modern techniques from social psychology is extremely sparse.¹⁷⁴ There has been a little bit of work considering whether people with strongly protective privacy views are systematically different than those with comparatively unprotective views.¹⁷⁵ Considering the

¹⁷⁰ Justice Scalia’s majority opinion indicates that the installation and use of a GPS tracker on a car would have been a trespass to chattels under common law precedents applicable at the time of the Founding. 132 S. Ct. at 949. Scalia analogizes 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. *Id.* at 950 n.3. Justice Alito makes his lack of fondness for Scalia’s analogy clear. *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.”).

¹⁷¹ See generally Orin S. Kerr, *An Equilibrium Adjustment Theory of the Fourth Amendment* 126 HARV. L. REV. 476 (2011).

¹⁷² *United States v. Karo*, 468 U.S. 705 (1984).

¹⁷³ See, e.g., Kugler, *supra* note 130, at 1.

¹⁷⁴ See, e.g., Stuart P. Green & Matthew B. Kugler, *When Is It Wrong to Trade Stocks on the Basis of Non-Public Information? Public Views of the Morality of Insider Trading*, 39 FORDHAM URB. L.J. 445 (2011); Margaret C. Stevenson & Tracy L. Caldwell, *Personality in Juror Decision-Making: Toward an Idiographic Approach in Research*, 33 LAW & PSYCHOL. REV. 93 (2009).

¹⁷⁵ See Sunil Hazari & 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 & Richard Divine, *Adolescents’ Concern for Privacy when Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors*, 35 FAMILY & CONSUMER SCI. RES. J. 232, 243-47 (2007); Mike Z. Yao et al., *Predicting User Concerns about Online Privacy*, 58 J. AM. SOC’Y FOR INFO. SCI. & TECH. 710, 718-20 (2007); Hoofnagle & Urban, *supra* note 106, at 261; Kugler, *supra* note 130, at 1; Alan F. Westin, “Whatever Works”--The American Public’s

unanimous result in *Jones*, however, it could be that the privacy ideologies relevant here work orthogonally to usual political ties. Moreover, if there are personality or other demographic factors that explain divergences in views about privacy law, then understanding those differences might enrich a legal realist perspective about why judges vote the way they do and how privacy may be regarded differently in 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 (with two minor changes) as the between subjects factor.¹⁷⁶ 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 6, there were no significant differences on this measure, though an inspection of the means suggests that those consistently low in privacy concern 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 conventions and norms.¹⁷⁷ 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.¹⁷⁸ 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.

Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues, in *Privacy and Self-Regulation in the Information Age* ch.1, §F (1997), available at <http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy>.

¹⁷⁶ 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.

¹⁷⁷ See Bob Altemeyer, *The Other “Authoritarian Personality,”* in 30 *ADVANCES IN EXPERIMENTAL SOCIAL PSYCHOLOGY* 47-92 (M. Zanna ed. 1998).

¹⁷⁸ 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.

Authoritarianism is one of the two major individual difference constructs in political psychology.¹⁷⁹ 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.¹⁸⁰ 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.¹⁸¹ 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.¹⁸² Past research has also shown that authoritarianism is one of the strongest predictors of attitudes toward both informational and decisional privacy issues.¹⁸³ This is unsurprising given the historical links between privacy protections and autonomy beliefs.¹⁸⁴

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.¹⁸⁵ The difference between the consistently high and consistently low groups was moderate, amounting to about half a standard deviation (Cohen's $d = .43$).¹⁸⁶ These results are supported by prior work showing that those high in authoritarianism are consistently less supportive of both information and decision privacy protections.¹⁸⁷ In fact, the same authoritarian submission scale here has previously displayed a

¹⁷⁹ See generally John Duckitt & 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, *supra* note 177, at 47.

¹⁸⁰ Herbert L. Mirels & Janet B. Dean, *Right-Wing Authoritarianism, Attitude Salience, and Beliefs about Matters of Fact*, *POL. PSYCH.* 839, 840-41 (2006) (reviewing studies).

¹⁸¹ See generally John Duckitt et al., *The Psychological Bases of Ideology and Prejudice: Testing A Dual Process Model*, 81 *J. PERSONALITY & SOC. PSYCH.* 75-93 (2002); Duckitt & Sibley, *supra* note 179, at 292.

¹⁸² 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 U.S. State Death Penalty Sentencing (1977-2004)*, 94 *J. PERSONALITY & SOC. PSYCH.* 913 (2008) (arguing that the directionality of a person's response to threat depends on their innate disposition, though authoritarian responding dominated overall).

¹⁸³ See Kugler, *supra* note 130, at 1.

¹⁸⁴ Louis Henkin, *Privacy and Autonomy*, 74 *COLUM. L. REV.* 1410, 1425 (1974)

¹⁸⁵ All posthoc tests described as significant are significant at least at the $p < .05$ level.

¹⁸⁶ 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.

¹⁸⁷ See Kugler, *supra* note 130, at 1.

moderate correlation with a composite of criminal procedure privacy questions.¹⁸⁸ This consistency across data collections underscores the role that authoritarianism plays in privacy attitudes.

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.¹⁸⁹ 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,¹⁹⁰ and highly conscientiousness respondents are more likely to be politically conservative.¹⁹¹ Extroversion has been positively linked to social popularity and number of parties attended, agreeableness and conscientiousness to honesty, and openness to musical inclination.¹⁹² Interestingly, a pessimistic view of one’s own intelligence is linked to high neuroticism even though undergraduate GPA is not.¹⁹³

The questionnaire battery we administered was specifically designed to be brief for use in mass-testing environments.¹⁹⁴ 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 6, there were significant differences across subject group on three of the measures: conscientiousness, extroversion, and neuroticism. Post-hoc tests revealed participants in the consistently low privacy concern 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 $d = .23$) That there was a relationship between extroversion and privacy attitudes is consistent with some prior research on the extraversion /

¹⁸⁸ *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.

¹⁸⁹ See generally COSTA, P. T., JR., & McCRAE, R. R., REVISED NEO PERSONALITY INVENTORY (NEO-PI-R) AND NEO FIVE- FACTOR INVENTORY (NEO-FFI) PROFESSIONAL MANUAL (1992); John, O. P., & Srivastava, S., *The Big Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives*, in HANDBOOK OF PERSONALITY: THEORY AND RESEARCH 102-138 (L.A. Pervin & O.P. John eds. 1999); Murray R. Barrick & Michael K. Mount, *The Big Five Personality Dimensions and Job Performance: A Meta-Analysis*, 44 PERSONNEL PSYCHOL. 1, 1–5 (1991).

¹⁹⁰ Baiyun Chen & 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 & 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).

¹⁹¹ Dana R. Carney et al., *The Secret Lives of Liberals and Conservatives: Personality Profiles, Interaction Styles, and the Things They Leave Behind*, 29 POL. PSYCHOL. 807, 824 (2008).

¹⁹² Paunonen, *supra* note 90, at 415-17.

¹⁹³ *Id.*

¹⁹⁴ Samuel D. Gosling et al., *A Very Brief Measure of the Big Five Personality Domains*. 37 J. RESEARCH IN PERSONALITY 504-528 (2003).

privacy nexus, however.¹⁹⁵ This relationship may suggest that, although those who didn't expect geolocation privacy are few in number, they are much more likely to have their views felt in social and political settings because extraverts advertise their views far more than do introverts. Observers may therefore assume that anti-privacy sentiment is more common than it actually is. This dynamic illustrates the dangers that might arise if judges assess popular expectations of privacy by talking only to their peers and assume that peer sentiment reflects popular sentiment; those who remain silent may be systematically different from those who speak up.

Table 6: Personality Characteristics as a Function of Privacy Views

	F (3,1229)	η^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 in the low privacy concern 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 $d = .20$). Additionally, those in the rising trend privacy concern group reported higher levels of conscientiousness than those in the middle group though, again, this effect was fairly small (Cohen's $d = .17$). There were no other significant differences on conscientiousness.

Subjects with low privacy concern reported lower levels of neuroticism than participants in the middle privacy concern (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 concern category.

¹⁹⁵ See Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2024-27 (2013).

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.¹⁹⁶ 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. 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 concern 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 $d = .39$). This finding cuts strongly against the conventional wisdom that younger cohorts do not care about their privacy.¹⁹⁷ At least when it comes to geolocation tracking, younger voters seem more inclined to view surveillance of any duration as constitutionally problematic. Older voters were more likely to cite the third party doctrine as the basis for their belief that sharing information with a third party entails an assumption that it can be shared with the government. By contrast, younger voters may have been acculturated during an area when sharing information with some acquaintances did not necessitate sharing it broadly.

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 even when compared to the others in the consistently low privacy concern group.¹⁹⁸ Those who endorse the third party doctrine were, on average, 58.45 years old ($SD = 15.62$). Those in the low privacy

¹⁹⁶ 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, available at <http://www.pewresearch.org/fact-tank/2015/05/14/dim-public-awareness-of-supreme-court-as-major-rulings-loom/> (visited July 10, 2015).

¹⁹⁷ See, e.g., Jo Bryce & 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 because of disinterest, insufficient awareness of the complexities of technology and data mining practices, and / or lack of understanding of legal protections."); Kashmir Hill, *Zuckerberg's Right: Young People Don't Care (as Much) About Privacy*, FORBES (Jan. 10, 2010), available at <http://www.forbes.com/sites/kashmirhill/2010/01/10/zuckerbergs-right-young-people-dont-care-as-much-about-privacy/>; But cf. Moscardelli & Divine, *supra* note 175, at 246 (finding teens had higher levels of privacy vigilance than adults, as reflected on temporally distant survey responses); Chris Jay Hoofnagle, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?*, at 20 (April 14, 2010 draft) available 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).

¹⁹⁸ $F(1,133) = 7.66, p = .006 \eta^2 = .054$.

group adopting other explanations were, on average, 50.57 (SD = 16.02). This is a moderate effect (Cohen's $d = .52$), and is coming on top of an already moderate age difference between the low privacy concern 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. Interestingly, there was no parallel difference on authoritarianism or Supreme Court knowledge.¹⁹⁹

E. Question Wording and the Robustness of Expectations

Any single formulation of a question is inherently limited and subject to criticism. Had we asked about 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.²⁰⁰ This sample was not census-representative. 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.²⁰¹ Our prediction was that the expectations manipulation would have no significant effect on participant responses. Based on prior research by Slobogin and Schumacher,²⁰² 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.

¹⁹⁹ Authoritarianism: $F(1,133) = .10, p = .758$. Supreme Court Knowledge: $F(1,133) = 1.41, p = .237$.

²⁰⁰ 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.

²⁰¹ 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.

²⁰² Slobogin & Schumacher, *supra* note 86, at 759.

Table 7: 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.²⁰³ The first vs. third person factor had the predicted effect, with more privacy violation reported for the first person wording.²⁰⁴ 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.²⁰⁵ There were no significant interactions between duration and the two experimental manipulations.

The analysis of the means therefore shows only one meaningful effect: more privacy (or expectations of privacy, or reasonable expectations of privacy) is being 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 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.²⁰⁶ There is a significant effect across first versus third person, however, such that there are more people in the consistently high category when the first person wording is used.²⁰⁷ This is consistent with a general increase in privacy expectations in the first person conditions.

²⁰³ $F(2, 1138) = 2.88, p = .06, \eta^2 = .005$. 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.

²⁰⁴ $F(2, 1138) = 15.93, p < .001, \eta^2 = .014$.

²⁰⁵ $F(1.74, 1977.26) = 143.51, p < .001, \eta^2 = .11$. 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).

²⁰⁶ Overall $\chi^2(10, 1144) = 12.735, p = .24$.

²⁰⁷ 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. $\chi^2(1, 1144) = 19.76, p < .001$.

Table 8: Consistency Categories as a Function of Experimental Conditions²⁰⁸

	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 note a vast difference between the baseline responses observed in our Mechanical Turk sample, which skews young and male, and our census-representative sample. Though Mechanical Turk is a convenient mechanism for data collection, these data suggest that it should not be used to establish base rates in the privacy domain; the demographic differences are simply too important. We would have suspected this based on the age effect observed in our representative sample, but these data confirm our concerns in a striking fashion.

F. Wave 3: Replication, Intrusiveness, and Suggestive Data on Other Searches.

Waves 1 and 2 left open three obvious areas for further exploration. One of these is simple replication. Are the privacy expectations measured here stable over time, or would results gathered mere weeks or months later differ? We know from the wave 1-wave 2 comparison that differences of a few weeks are likely not relevant – those waves were indistinguishable even though the *Reilly* decision was handed down in the interim. But what about the space of a year?

Another area of expansion relates our expectation data to the intrusiveness data collected by Slobogin in his various studies. We have shown that expectations vary little as search duration increases. Is the same also true of the perceived intrusiveness of a search? If not, this may implicate the post-Katz reasonableness analysis as well as Kerr’s policy model.

²⁰⁸ Compare the responses reported in Tables 1 and 2 (nationally representative sample) to the much more privacy protective responses reported in Tables 7 and 8 (Mechanical Turk sample). 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. The same numbers for the identically worded question (3rd 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 13). 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%.

Finally, it is worth calibrating our expectations data in the GPS monitoring context by comparing it to data from other, related contexts. What do privacy expectations look like in the domain of cell site monitoring? Or use of facial recognition technology?

In part to answer these questions, a third wave of data collection was conducted between May 26 and June 2, 2015, approximately a year after waves one and two. Participants for this wave were also recruited by Toluna. The final sample contained 1441 respondents, all of whom were adult US Citizens.²⁰⁹ The median age was 46 (range 18-89, $M = 46.04$, $SD = 16.41$). 49.8% of the sample was female. Slightly more of the sample than the national population as a whole had completed at least some college coursework, but otherwise the educational attainment of the sample was roughly equivalent to that of the broader population.²¹⁰ 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. When asked to rate their political orientation on a scale ranging from 1 – Very Liberal to 7 – Very Conservative, the mean response was 4.19 ($SD = 1.78$), indicating a politically moderate sample.

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 5 point response scale. The only difference between the questions of waves 1 and 2 and those of the new wave is that the new wave's employed a slightly revised version of the locate question. It now read "Used a car's onboard GPS system to locate it on public streets without the owner's permission?" We believe that this is somewhat clearer than the earlier version.²¹¹

As can be seen in Table 9, the results of each wave are nearly identical. There are no significant differences in the means or the consistency categories.

²⁰⁹ 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.

²¹⁰ In the sample, 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.

²¹¹ As mentioned above in note 201, both versions were used in the wording test study and the results did not differ.

Table 9: Consistency Between 2014 and 2015 Waves.

	Waves I and II	Wave III
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%

	Waves I and II			Wave III		
	Mean	% Below	% Above	Mean	% 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%

This data should therefore help to alleviate concerns that privacy attitudes will not be consistent over time. Even after a year, a year that included any number of events arguably relevant to police-community relations,²¹² almost nothing has changed.

The second version of the GPS tracking question asked three questions designed to assess the intrusiveness of GPS tracking rather than expectations. The wording of these is as below:

- 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?
- If law enforcement used a car's onboard GPS system to track its movements on public streets for one day without the owner's permission.
 - Questions repeat.
- Same, but for one week.
- Same, but for one month.

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.²¹³ All response scales ranged from 1 – Not at All to 5 – Very, with no labels on the

²¹² See, for example, Michael S. Schmidt & Matt Apuzzo, *South Carolina Officer Is Charged With the Murder of Walter Scott*, N.Y. TIMES, April 8, 2015, at A1.

²¹³ See Kugler, *supra* note 86, at 1194 (using these as measures of the privacy and dignity interests implicated by border searches of electronic devices).

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.” Whether “only somewhat embarrassing” is embarrassing enough to be of legal significance is, of course, a policy question.

These data followed a somewhat different pattern. As can be seen in Table 10, there are larger shifts on these measures 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 .45.²¹⁴

Table 10: Mean Intrusiveness, Information, and Embarrassment Scores For Each Duration of Search

		Mean		% 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%

As can be seen in Table 11, this increased salience for duration had some effect on the consistency categories. 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%).²¹⁵

²¹⁴ 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.

²¹⁵ Intrusiveness: $\chi^2(1, 747) = 13.51, p < .001$. Information: $\chi^2(1, 747) = 22.81, p < .001$. Embarrassment: $\chi^2(1, 747) = 10.88, p < .001$.

Table 11: 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%

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

Table 12: 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)

Table 12 contains the data from these 101 point scales. There are several takeaways. 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.²¹⁶ 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

²¹⁶ 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.

implement the mosaic theory's duration distinction because many of them have attempted to draw a line in precisely this place.

The intrusiveness, information, and embarrassment scores do support distinguishing searches of a moment from searches of a month, however. Under our theory, consideration of this distinction should occur after the *Katz* prong 1 determination that the Fourth Amendment is potentially implicated. They would be germane to the "private facts" analysis that unfolds as part of *Katz* prong 2.

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 for the GPS tracking questions in the waves 1 and 2 and given to some participants in wave 3. Though these results are not central to our project, they provide a sense of how the rule we advocate in the GPS monitoring context would affect the handling of other hot-button Fourth Amendment questions.

Table 13: Results for Other Searches

	Mean	% Above	% Below	Ratio: Above/Below
Remote Activate Webcam ²¹⁷	4.06 (1.37)	73%	15%	4.74
Obtain Emails From ISP	3.73 (1.40)	63%	20%	3.16
Stingray Cellphone 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%	0.63
Camera In Public Park	2.40 (1.55)	29%	58%	0.49

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*,²¹⁸ were exactly evenly split with as many people expecting privacy as not. On tracking a person using cell site data, on the other

²¹⁷ The exact wording of each scenario is below. They appeared in random order. Participants were asked if it would 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?

²¹⁸ 135 S. Ct. 2443 (2015).

hand, about half the participants thought this was a violation of their expectations of privacy, and just under a third 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 a person'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.²¹⁹ An overwhelming majority also feels that the police obtaining emails from an Internet Service Provider infringed a reasonable expectation of privacy. Federal law generally requires police to obtain a warrant to access recent email communications,²²⁰ and one circuit court has ruled that the Fourth Amendment also requires the police to obtain a warrant in order to obtain any emails from an Internet Service Provider.²²¹ 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. The case law is consistent with popular sentiment here as well.²²²

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 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 consistent privacy concern. 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 problematic" 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.

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

²¹⁹ See *Clements-Jeffrey v. City of Springfield*, 810 F. Supp.2d 857, 865-66, 874-77 (S.D. Ohio 2011).

²²⁰ See, e.g., 18 U.S.C. § 2703 (Stored Communications Act warrant requirement); 18 U.S.C. § 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 U.S.C. § 2703(b)

²²¹ See *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (finding a reasonable expectation of privacy in email contents).

²²² See, e.g., *United States v. Brooks*, 911 F. Supp.2d 836, 842-43 (D. Ariz. 2012).

personality scale correlate with expectations of information privacy in police search contexts. Other psychological orientations, like the Big Five extraversion scale, are also useful in predicting individuals' responses to real-world investigation scenarios. Still other demographic variables, like age, plausibly drive the resonance of some doctrines, the third-party-doctrine in particular. This paper is an important first step toward the broader goal of explaining the psychological basis 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. 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 expect²²³ – 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. We argue that such data can and should be one critical tool for resolving questions under the *Katz* Court's reasonable expectation of privacy test.

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 render the theory bad law? We believe that is a difficult question, but we are inclined to answer "yes." We were initially persuaded by the sentiment voiced by jurists like Judge Ginsburg and Justice Alito that the whole is greater than the sum of its parts when it comes to information privacy. But this idea's failure to resonate with the public presents a 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. It is a problem when Fourth Amendment protections and popular expectations are misaligned because people are then guarded when they should feel free and feel free when they should be guarded. Liberty is senselessly diminished and people needlessly self-censor when they underestimate legal protections for privacy. Privacy is needlessly invaded and people take inadequate precautions when they overestimate the law's protection for privacy. The mosaic theory's most prominent academic critic has emphasized how difficult it would be for courts to operationalize its implications as Fourth Amendment doctrine.²²⁴ Our research identifies an even more troubling concern – the private citizens whose behavior is to be influenced by the Fourth Amendment largely regard the mosaic theory as non-intuitive and perhaps even unintelligible.

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

²²³ See *supra* note 53; cf. *Minnesota v. Carter*, 525 U.S. 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).

²²⁴ Kerr, *supra* note 6, at 328-343, 346-348.

would be largely futile. While a sufficiently determined campaign might make strides over time, we are skeptical.

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, and the harm to legitimacy is also likely real, if difficult to quantify. 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 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,²²⁵ 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 expect” or “this is what my law clerk expects” being used as a proxy for what members of society generally expect and value. If the courts are to ignore actual laypeople’s expectations of privacy as a factor relevant to the *Katz* inquiry, then the “reasonable expectations of privacy” test deserves a candid renaming, and the largely inattentive American public deserves an explanation for why their expectations are not deemed relevant.

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. Under our method, popular expectations assessed via rigorous social science techniques would become a key part of the Fourth Amendment inquiry, displacing the courts’ presently inconsistent approach to *Katz* prong 1. An exploration of these expectations would not be the only relevant consideration – courts would still explore existing precedents and common law limitations as part of *Katz* step zero, and they will still examine the sensitivity of the information at issue in *Katz* prong 2. In short, we propose a system whereby courts do in a regular and organized manner what they currently do ad hoc, and where they use empirical social science to do much better what was previously left to bare intuition.

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 non-search. 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 the mosaic theory fails miserably as a descriptive account of what people expect from law enforcement. We are concerned enough by this disconnect 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.

²²⁵ See, e.g., Dahlia Lithwick, *The 2014 Supreme Court: An Ivy League Clan*, NEW REPUBLIC (Nov. 13, 2014), available at <http://www.newrepublic.com/article/120173/2014-supreme-court-ivy-league-clan-disconnected-reality>

Readers with comments should address them to:

Professor Lior Strahilevitz
lior@uchicago.edu

Chicago Working Papers in Law and Economics
(Second Series)

For a listing of papers 1–600 please go to Working Papers at
<http://www.law.uchicago.edu/Lawecon/index.html>

601. David A. Weisbach, Should Environmental Taxes Be Precautionary? June 2012
602. Saul Levmore, Harmonization, Preferences, and the Calculus of Consent in Commercial and Other Law, June 2012
603. David S. Evans, Excessive Litigation by Business Users of Free Platform Services, June 2012
604. Ariel Porat, Mistake under the Common European Sales Law, June 2012
605. Stephen J. Choi, Mitu Gulati, and Eric A. Posner, The Dynamics of Contrat Evolution, June 2012
606. Eric A. Posner and David Weisbach, International Paretianism: A Defense, July 2012
607. Eric A. Posner, The Institutional Structure of Immigration Law, July 2012
608. Lior Jacob Strahilevitz, Absolute Preferences *and* Relative Preferences in Property Law, July 2012
609. Eric A. Posner and Alan O. Sykes, International Law and the Limits of Macroeconomic Cooperation, July 2012
610. M. Todd Henderson and Frederick Tung, Reverse Regulatory Arbitrage: An Auction Approach to Regulatory Assignments, August 2012
611. Joseph Isenbergh, Cliff Schmitt, August 2012
612. James Melton and Tom Ginsburg, Does De Jure Judicial Independence Really Matter?, September 2014
613. M. Todd Henderson, Voice versus Exit in Health Care Policy, October 2012
614. Gary Becker, François Ewald, and Bernard Harcourt, “Becker on Ewald on Foucault on Becker” American Neoliberalism and Michel Foucault’s 1979 *Birth of Biopolitics* Lectures, October 2012
615. William H. J. Hubbard, Another Look at the Eurobarometer Surveys, October 2012
616. Lee Anne Fennell, Resource Access Costs, October 2012
617. Ariel Porat, Negligence Liability for Non-Negligent Behavior, November 2012
618. William A. Birdthistle and M. Todd Henderson, Becoming the Fifth Branch, November 2012
619. David S. Evans and Elisa V. Mariscal, The Role of Keyword Advertisign in Competition among Rival Brands, November 2012
620. Rosa M. Abrantes-Metz and David S. Evans, Replacing the LIBOR with a Transparent and Reliable Index of interbank Borrowing: Comments on the Wheatley Review of LIBOR Initial Discussion Paper, November 2012
621. Reid Thompson and David Weisbach, Attributes of Ownership, November 2012
622. Eric A. Posner, Balance-of-Powers Arguments and the Structural Constitution, November 2012
623. David S. Evans and Richard Schmalensee, The Antitrust Analysis of Multi-Sided Platform Businesses, December 2012
624. James Melton, Zachary Elkins, Tom Ginsburg, and Kalev Leetaru, On the Interpretability of Law: Lessons from the Decoding of National Constitutions, December 2012
625. Jonathan S. Masur and Eric A. Posner, Unemployment and Regulatory Policy, December 2012
626. David S. Evans, Economics of Vertical Restraints for Multi-Sided Platforms, January 2013
627. David S. Evans, Attention to Rivalry among Online Platforms and Its Implications for Antitrust Analysis, January 2013
628. Omri Ben-Shahar, Arbitration and Access to Justice: Economic Analysis, January 2013
629. M. Todd Henderson, Can Lawyers Stay in the Driver’s Seat?, January 2013
630. Stephen J. Choi, Mitu Gulati, and Eric A. Posner, Altruism Exchanges and the Kidney Shortage, January 2013
631. Randal C. Picker, Access and the Public Domain, February 2013
632. Adam B. Cox and Thomas J. Miles, Policing Immigration, February 2013
633. Anup Malani and Jonathan S. Masur, Raising the Stakes in Patent Cases, February 2013
634. Ariel Porat and Lior Strahilevitz, Personalizing Default Rules and Disclosure with Big Data, February 2013
635. Douglas G. Baird and Anthony J. Casey, Bankruptcy Step Zero, February 2013
636. Oren Bar-Gill and Omri Ben-Shahar, No Contract? March 2013
637. Lior Jacob Strahilevitz, Toward a Positive Theory of Privacy Law, March 2013
638. M. Todd Henderson, Self-Regulation for the Mortgage Industry, March 2013
639. Lisa Bernstein, Merchant Law in a Modern Economy, April 2013
640. Omri Ben-Shahar, Regulation through Boilerplate: An Apologia, April 2013

- 641. Anthony J. Casey and Andres Sawicki, Copyright in Teams, May 2013
- 642. William H. J. Hubbard, An Empirical Study of the Effect of *Shady Grove v. Allstate* on Forum Shopping in the New York Courts, May 2013
- 643. Eric A. Posner and E. Glen Weyl, Quadratic Vote Buying as Efficient Corporate Governance, May 2013
- 644. Dhammika Dharmapala, Nuno Garoupa, and Richard H. McAdams, Punitive Police? Agency Costs, Law Enforcement, and Criminal Procedure, April 2015
- 645. Tom Ginsburg, Jonathan S. Masur, and Richard H. McAdams, Libertarian Paternalism, Path Dependence, and Temporary Law, June 2013
- 646. Stephen M. Bainbridge and M. Todd Henderson, Boards-R-Us: Reconceptualizing Corporate Boards, July 2013
- 647. Mary Anne Case, Is There a Lingua Franca for the American Legal Academy? July 2013
- 648. Bernard Harcourt, Beccaria's *On Crimes and Punishments*: A Mirror of the History of the Foundations of Modern Criminal Law, July 2013
- 649. Christopher Buccafusco and Jonathan S. Masur, Innovation and Incarceration: An Economic Analysis of Criminal Intellectual Property Law, July 2013
- 650. Rosalind Dixon & Tom Ginsburg, The South African Constitutional Court and Socio-economic Rights as "Insurance Swaps", August 2013
- 651. Maciej H. Kotowski, David A. Weisbach, and Richard J. Zeckhauser, Audits as Signals, August 2013
- 652. Elisabeth J. Moyer, Michael D. Woolley, Michael J. Glotter, and David A. Weisbach, Climate Impacts on Economic Growth as Drivers of Uncertainty in the Social Cost of Carbon, August 2013
- 653. Eric A. Posner and E. Glen Weyl, A Solution to the Collective Action Problem in Corporate Reorganization, September 2013
- 654. Gary Becker, François Ewald, and Bernard Harcourt, "Becker and Foucault on Crime and Punishment"—A Conversation with Gary Becker, François Ewald, and Bernard Harcourt: The Second Session, September 2013
- 655. Edward R. Morrison, Arpit Gupta, Lenora M. Olson, Lawrence J. Cook, and Heather Keenan, Health and Financial Fragility: Evidence from Automobile Crashes and Consumer Bankruptcy, October 2013
- 656. Evidentiary Privileges in International Arbitration, Richard M. Mosk and Tom Ginsburg, October 2013
- 657. Voting Squared: Quadratic Voting in Democratic Politics, Eric A. Posner and E. Glen Weyl, October 2013
- 658. The Impact of the U.S. Debit Card Interchange Fee Regulation on Consumer Welfare: An Event Study Analysis, David S. Evans, Howard Chang, and Steven Joyce, October 2013
- 659. Lee Anne Fennell, Just Enough, October 2013
- 660. Benefit-Cost Paradigms in Financial Regulation, Eric A. Posner and E. Glen Weyl, April 2014
- 661. Free at Last? Judicial Discretion and Racial Disparities in Federal Sentencing, Crystal S. Yang, October 2013
- 662. Have Inter-Judge Sentencing Disparities Increased in an Advisory Guidelines Regime? Evidence from Booker, Crystal S. Yang, March 2014
- 663. William H. J. Hubbard, A Fresh Look at Plausibility Pleading, March 2015
- 664. Tom Ginsburg, Nick Foti, and Daniel Rockmore, "We the Peoples": The Global Origins of Constitutional Preambles, April 2014
- 665. Lee Anne Fennell and Eduardo M. Peñalver, Exactions Creep, December 2013
- 666. Lee Anne Fennell, Forcings, December 2013
- 667. Stephen J. Choi, Mitu Gulati, and Eric A. Posner, A Winner's Curse?: Promotions from the Lower Federal Courts, December 2013
- 668. Jose Antonio Cheibub, Zachary Elkins, and Tom Ginsburg, Beyond Presidentialism and Parliamentarism, December 2013
- 669. Lisa Bernstein, Trade Usage in the Courts: The Flawed Conceptual and Evidentiary Basis of Article 2's Incorporation Strategy, November 2013
- 670. Roger Allan Ford, Patent Invalidity versus Noninfringement, December 2013
- 671. M. Todd Henderson and William H.J. Hubbard, Do Judges Follow the Law? An Empirical Test of Congressional Control over Judicial Behavior, January 2014
- 672. Lisa Bernstein, Copying and Context: Tying as a Solution to the Lack of Intellectual Property Protection of Contract Terms, January 2014

673. Eric A. Posner and Alan O. Sykes, Voting Rules in International Organizations, January 2014
674. Tom Ginsburg and Thomas J. Miles, The Teaching/Research Tradeoff in Law: Data from the Right Tail, February 2014
675. Ariel Porat and Eric Posner, Offsetting Benefits, February 2014
676. Nuno Garoupa and Tom Ginsburg, Judicial Roles in Nonjudicial Functions, February 2014
677. Matthew B. Kugler, The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study, February 2014
678. David S. Evans, Vanessa Yanhua Zhang, and Xinzhu Zhang, Assessing Unfair Pricing under China's Anti-Monopoly Law for Innovation-Intensive Industries, March 2014
679. Jonathan S. Masur and Lisa Larrimore Ouellette, Deference Mistakes, March 2014
680. Omri Ben-Shahar and Carl E. Schneider, The Futility of Cost Benefit Analysis in Financial Disclosure Regulation, March 2014
681. Yun-chien Chang and Lee Anne Fennell, Partition and Revelation, April 2014
682. Tom Ginsburg and James Melton, Does the Constitutional Amendment Rule Matter at All? Amendment Cultures and the Challenges of Measuring Amendment Difficulty, May 2014
683. Eric A. Posner and E. Glen Weyl, Cost-Benefit Analysis of Financial Regulations: A Response to Criticisms, May 2014
684. Adam B. Badawi and Anthony J. Casey, The Fannie and Freddie Bailouts Through the Corporate Lens, March 2014
685. David S. Evans, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms, April 2014
686. Preston M. Torbert, A Study of the Risks of Contract Ambiguity, May 2014
687. Adam S. Chilton, The Laws of War and Public Opinion: An Experimental Study, May 2014
688. Robert Cooter and Ariel Porat, Disgorgement Damages for Accidents, April 2015
689. David Weisbach, Distributionally-Weighted Cost Benefit Analysis: Welfare Economics Meets Organizational Design, June 2014
690. Robert Cooter and Ariel Porat, Lapses of Attention in Medical Malpractice and Road Accidents, June 2014
691. William H. J. Hubbard, Nuisance Suits, June 2014
692. Saul Levmore & Ariel Porat, Credible Threats, July 2014
693. Douglas G. Baird, One-and-a-Half Badges of Fraud, August 2014
694. Adam Chilton and Mila Versteeg, Do Constitutional Rights Make a Difference? August 2014
695. Maria Bigoni, Stefania Bortolotti, Francesco Parisi, and Ariel Porat, Unbundling Efficient Breach, August 2014
696. Adam S. Chilton and Eric A. Posner, An Empirical Study of Political Bias in Legal Scholarship, August 2014
697. David A. Weisbach, The Use of Neutralities in International Tax Policy, August 2014
698. Eric A. Posner, How Do Bank Regulators Determine Capital Adequacy Requirements? September 2014
699. Saul Levmore, Inequality in the Twenty-First Century, August 2014
700. Adam S. Chilton, Reconsidering the Motivations of the United States? Bilateral Investment Treaty Program, July 2014
701. Dhammika Dharmapala and Vikramaditya S. Khanna, The Costs and Benefits of Mandatory Securities Regulation: Evidence from Market Reactions to the JOBS Act of 2012, August 2014
702. Dhammika Dharmapala, What Do We Know About Base Erosion and Profit Shifting? A Review of the Empirical Literature, September 2014
703. Dhammika Dharmapala, Base Erosion and Profit Shifting: A Simple Conceptual Framework, September 2014
704. Lee Anne Fennell and Richard H. McAdams, Fairness in Law and Economics: Introduction, October 2014
705. Thomas J. Miles and Adam B. Cox, Does Immigration Enforcement Reduce Crime? Evidence from 'Secure Communities', October 2014
706. Ariel Porat and Omri Yadlin, A Welfarist Perspective on Lies, May 2015
707. John Bronsteen, Christopher Buccafusco and Jonathan S. Masur, Well-Being and Public Policy, November 2014
708. David S. Evans, The Antitrust Analysis of Rules and Standards for Software Platforms, November 2014
709. E. Glen Weyl and Alexander White, Let the Best 'One' Win: Policy Lessons from the New Economics of Platforms, December 2014

- 710. Lee Anne Fennell, Agglomerama, December 2014
- 711. Anthony J. Casey and Aziz Z. Huq, The Article III Problem in Bankruptcy, December 2014
- 712. Adam S. Chilton and Mila Versteeg, The Inefficacy of Constitutional Torture Prohibitions, December 2014
- 713. Lee Anne Fennell and Richard H. McAdams, The Distributive Deficit in Law and Economics, January 2015
- 714. Omri Ben-Shahar and Kyle D. Logue, The Perverse Effects of Subsidized Weather Insurance, May 2015
- 715. Adam M. Samaha and Lior Jacob Strahilevitz, Don't Ask, Must Tell—and Other Combinations, January 2015
- 716. Jonathan S. Masur and Eric A. Posner, Toward a Pigovian State, February 2015
- 717. Lee Fennell, Slicing Spontaneity, February 2015
- 718. Steven Douglas Smith, Michael B. Rappaport, William Baude, and Stephen E. Sachs, The New and Old Originalism: A Discussion, February 2015
- 719. Adam S. Chilton and Eric A. Posner, The Influence of History on States' Compliance with Human Rights Obligations, March 2015
- 720. Saul Levmore and Ariel Porat, No-Haggle Agreements, March 2015
- 721. Saul Levmore and Ariel Porat, Rethinking Threats, March 2015
- 722. Adam Chilton, The Politics of the United States' Bilateral Investment Treaty Program, March 2015
- 723. David S. Evans and Alexis Pirchio, An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most, March 2015
- 724. Anthony J. Casey and Eric A. Posner, A Framework for Bailout Regulation, February 2015
- 725. Mihir A. Desai and Dhammika Dharmapala, Interest Deductions in a Multijurisdictional World, April 2015
- 726. Eric A. Posner, The Law, Economics, and Psychology of Manipulation, June 2015
- 727. Matthew B. Kugler and Lior Jacob Strahilevitz, Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory, July 2015