Printed in U.S.A.
Vol. 111, No. 1

KNOWLEDGE AND FOURTH AMENDMENT PRIVACY

Matthew Tokson

ABSTRACT—This Article examines the central role that knowledge plays in determining the Fourth Amendment's scope. What people know about surveillance practices or new technologies often shapes the "reasonable expectations of privacy" that define the Fourth Amendment's boundaries. From early decisions dealing with automobile searches to recent cases involving advanced information technologies, courts have relied on assessments of knowledge in a wide variety of Fourth Amendment contexts. Yet the analysis of knowledge in Fourth Amendment law is rarely if ever studied on its own.

This Article fills that gap. It starts by identifying the characteristics of Fourth Amendment knowledge. It finds, for instance, that courts typically look to societal knowledge rather than individual knowledge, allowing them to establish broad precedents to govern police behavior.

The Article then draws on communications scholarship and research on the spread of innovations to identify conceptual problems inherent in assessing societal knowledge. It also uses original empirical evidence to evaluate courts' claims regarding societal knowledge in a variety of important cases. And it contends that a knowledge-based Fourth Amendment will shrink and weaken over time as public awareness of new technologies and threats to privacy continues to grow.

In light of these findings, the Article proposes that the knowledge inquiry in Fourth Amendment law, and the reasonable expectation of privacy test with which it is intertwined, be replaced with a legal regime better able to adjust to technological and social change. The Article offers two alternatives, one based on existing laws and property concepts, and the other based on direct normative balancing of the benefits and harms of new surveillance practices. It analyzes the strengths and weaknesses of these alternatives, with the goal of developing a Fourth Amendment regime that can effectively protect privacy in novel technological and social contexts.

AUTHOR—Assistant Professor, Salmon P. Chase College of Law, Northern Kentucky University. Thanks to Eric Alden, Will Baude, Bryan Choi, Ursula Doyle, Daniel Epps, Chad Flanders, Jack Harrison, Orin Kerr, Jennifer Kinsley, Cynthia Lee, Judson Littleton, Michael Mannheimer, Dina Mishra, Laurent Sacharoff, Ric Simmons, Lior Strahilevitz, Barbara

Wagner, and all participants in the CrimFest Conference, Midwestern Privacy Law Scholars Workshop, Privacy Law Scholars Conference, Saint Louis University faculty workshop, and the Chase faculty workshop for helpful comments and suggestions. Special thanks to Carol Bredemeyer for excellent research assistance.

INTRODUCTION

Roughly ninety-one percent of American adults own a cell phone.[1] Suppose that one of these Americans, John, is a typical cell phone user. He takes his phone with him everywhere and uses it regularly. He gives little thought to how exactly cell phones work. One day, John hears a disturbing news report on the radio. It describes how cell phone companies constantly record users' locations using their cell phone signals.[2] If John continues to use his cell phone, has he knowingly waived any Fourth Amendment right to privacy in his location? More broadly, how should courts assess what people know about their privacy? And how does that knowledge relate to the "reasonable expectations of privacy" that define the Fourth Amendment's scope?[3]

This Article addresses these issues and examines the central role that knowledge plays in setting the boundaries of Fourth Amendment protection. Courts have relied on assessments of knowledge in a wide variety of Fourth Amendment contexts, from early post-*Katz* decisions dealing with automobile searches to recent cases involving advanced information technologies and surveillance practices.[4] Indeed, evaluating knowledge is typically crucial to determining people's reasonable expectations of privacy. Yet the concept of knowledge in Fourth Amendment law is rarely if ever studied on its own.[5]

This Article identifies several characteristics of the knowledge inquiry, although courts' examination of knowledge in Fourth Amendment cases is hardly straightforward or uniform. First, courts generally look to what a person should know about privacy-relevant information, rather than

---

[1] LEE RAINIE, PEW RESEARCH CTR., CELL PHONE OWNERSHIP HITS 91% OF ADULTS, (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults [https://perma.cc/2MUZ-GVBL].

[2] This is indeed the case, as explained below in Section II.E.1. Episode Five of NPR's radio series "Serial" discussed the use of cell phone company records to determine a person's location. *See Serial: Route Talk*, NPR (Oct. 23, 2014), https://serialpodcast.org/season-one/5/route-talk.

[3] *See, e.g.*, Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (discussing the Fourth Amendment's scope by reference to a citizen's "reasonable expectation of privacy").

[4] *See infra* Part II.

[5] The lengthiest discussions of Fourth Amendment knowledge of which I am aware can be found in Mary Graw Leary, Katz *on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 377–80 (2013) and Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588–90 (2009). *See also* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 388–89 (2006) (discussing the various ways courts have treated the question of what privacy cell phone users can reasonably expect in their location information). I critique the treatment of knowledge in the Fourth Amendment literature in Section II.B, *infra*.

what she actually knows.[6] Second, courts typically do this by reaching a conclusion about the collective knowledge possessed by society, or "societal knowledge," and then attributing that knowledge to the individual citizen.[7] They look to societal knowledge both when examining knowing exposure to the public and when considering reasonable expectations of privacy in general.[8] And judges tend to evaluate societal knowledge based on their own knowledge or intuition rather than using empirical evidence, which is often unavailable.[9]

Using societal knowledge to anchor the Fourth Amendment inquiry has several advantages for courts. It allows them to avoid particularized fact-finding about each citizen's mental state and to establish broad precedents to govern police behavior. Measuring knowledge in the present day can also help courts determine future expectations, since, as a general matter, our predictions for the future depend on our understanding of the present.

Yet any assessment of societal knowledge presents conceptual difficulties. Innovation and communications research, for example, recognizes that knowledge is not a simple, binary concept but rather a multistep process that is intrinsically difficult to measure.[10] Mere awareness is not the same as basic comprehension, and basic comprehension differs from deep understanding. Courts' failures to recognize this complexity may lead them to assume significant societal knowledge where only minimal awareness exists.[11] Further, assuming meaningful levels of societal knowledge is dangerous when most citizens will rationally remain ignorant of many aspects of public policy, technology, and criminal justice.[12] Obtaining detailed knowledge about these topics is costly, and most people have little use for such information. Knowledge also tends to spread unevenly across populations and is often slowest to reach people with lower levels of education and social status.[13] This may raise issues of fundamental fairness when courts attribute the knowledge of the median citizen to individuals with below-median levels of education or wealth.

These difficulties have led judges to reach erroneous conclusions about societal knowledge in a variety of important Fourth Amendment

---

[6] *See infra* Section II.A.

[7] *See infra* Section II.A.

[8] *See infra* Sections II.B–II.C.

[9] *See infra* Section III.B.

[10] *See* discussion *infra* Section III.A.1.

[11] *See infra* Section III.A.1.

[12] *See infra* Section III.A.3.

[13] *See infra* Section III.A.4.

cases.[14] Judges' faulty conclusions about knowledge may stem from their failure to recognize the multilayered nature of societal knowledge, or from hindsight bias and the human tendency to impute one's knowledge to others.[15] Whatever the reason, courts' reliance on empirically incorrect findings about societal knowledge is unsustainable.

Moreover, even if courts could assess societal knowledge with perfect accuracy, tying the Fourth Amendment's scope to such knowledge carries serious downsides. The domain of a knowledge-based Fourth Amendment is likely to shrink over time, as an increasingly intelligent, educated, and technologically adept population learns about new technologies and threats to privacy.[16] In the meantime, such a regime is inherently unstable, subject to unpredictable spikes in public awareness caused by high-salience news events or government leaks.[17] A knowledge-based Fourth Amendment also impedes antisurveillance political advocacy, because educating citizens about privacy threats can lead to reduced constitutional protection.

In light of these disadvantages, this Article proposes that the knowledge inquiry in Fourth Amendment law, and the reasonable expectation of privacy test with which it is intertwined, be replaced by a legal regime that is better able to adjust to technological and social change. Building on existing case law[18] and scholarship,[19] I offer two alternatives to a knowledge-centered view of the Fourth Amendment. The first is based on existing laws and property concepts, and brings the institutional advantages of legislatures to bear on novel technological issues.[20] Such a regime could maximize predictability and clarity while increasing the stability of Fourth Amendment protection. The second calls for courts to engage in a direct normative balancing of the benefits and harms of new surveillance practices, using a test focusing on the most significant and measureable factors in this balance.[21] This approach could maximize adaptability to new

---

[14] *See infra* Section III.A.3.

[15] *See infra* Sections III.A.1–III.B.2.

[16] *See infra* Section IV.C.

[17] *See infra* Section IV.B.

[18] *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality opinion) (finding the defendant had no reasonable expectation of privacy as to the contents of a partially uncovered greenhouse when an officer observed marijuana growing from a low-flying helicopter in public airspace); Hudson v. Palmer, 468 U.S. 517, 526–27 (1984) (describing the security issues unique to prisons and describing the analysis of the reasonable expectation of privacy as "necessarily entail[ing] a balancing of interests" between those security concerns and individuals' privacy).

[19] *See, e.g.*, Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 507–22 (2007); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

[20] *See infra* Section V.B.

[21] *See infra* Section V.C.

technologies and prevent the erosion of the Fourth Amendment as societal knowledge increases.

The Article examines the strengths and weaknesses of these alternatives relative to each other and to current law. Ultimately, the goal of this discussion is to develop a Fourth Amendment regime that can effectively protect privacy in novel technological and social contexts.

Part I of this Article discusses the general history and nature of the test, established in *Katz*, that currently governs Fourth Amendment scope. Part II explores how courts rely on assessments of societal knowledge to decide a wide variety of Fourth Amendment questions. Part III examines the conceptual and practical difficulties of measuring societal knowledge. It also reports the results of an original survey of cell phone users that measured users' knowledge of cell phone surveillance techniques. It then compares the results to those intuited by judges in cell phone surveillance cases. Part IV discusses the instability of a knowledge-based Fourth Amendment regime and the potential for erosion over time as public knowledge of surveillance grows. Part V offers alternative approaches for determining the Fourth Amendment's scope and explores the strengths and weaknesses of each alternative.

I. THE *KATZ* TEST

The law governing the Fourth Amendment's scope is not a model of clarity. It has been criticized as confusing,[22] illogical,[23] chaotic,[24] and inconsistent across cases.[25] Yet the contours of the test for Fourth Amendment coverage are relatively well-defined.[26] This Part briefly describes this test and the current state of Fourth Amendment law.

A. Development of the Katz *Test*

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[27] The Supreme Court has generally interpreted

---

[22] Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149–50 (1998).

[23] Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1321 (1981).

[24] Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1208 (1985).

[25] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511–12 (2010).

[26] *See* Oliver v. United States, 466 U.S. 170, 177–78 (1984).

[27] U.S. CONST. amend. IV.

the Fourth Amendment's reasonableness standard to require that the government obtain a warrant prior to searching or seizing.[28]

The scope of the Fourth Amendment is potentially very broad, covering all searches and seizures of "persons, houses, papers, and effects." But the Constitution offers no definition of what a "search" (or a "seizure") is for Fourth Amendment purposes, and there is no direct history on the subject.[29] In general, a search can be any examination of any thing—"[a]n enquiry, an examination, the act of seeking," as a Founding Era dictionary put it,[30] or "scrutiny for the purpose of finding a person or thing [or the] investigation of a question," as a modern dictionary defines it.[31] The Supreme Court has never required that the police obtain a warrant before seeking any information or object, a mandate that would severely disable the practice of law enforcement. The Court has always defined "search" far more narrowly.[32]

In its pre-*Katz* Fourth Amendment cases, the Court limited the coverage of the Fourth Amendment to "material things"[33] and "constitutionally protected area[s]."[34] Accordingly, in a landmark 1928 case, *Olmstead v. United States*, the Court held that government officers did not conduct a "search" when they tapped Olmstead's telephone lines and listened to his conversations for several months.[35] The conversations were not material things like "papers" or "effects" and the officers therefore committed no trespass on Olmstead's property when they tapped the public telephone wires.[36]

---

[28] *E.g.*, Weeks v. United States, 232 U.S. 383, 393 (1914), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961). There are several exceptions to the warrant requirement, including exceptions for automobiles, *Carroll v. United States*, 267 U.S. 132, 153 (1925), exigent circumstances, *Warden v. Hayden*, 387 U.S. 294, 298–99 (1967) (citing *McDonald v. United States*, 335 U.S. 451, 456 (1948)), and searches incident to arrest, *Chimel v. California*, 395 U.S. 752, 762–63 (1969).

[29] *See* U.S. CONST. amend. IV; *see also* Luis G. Stelzner, *The Fourth Amendment: The Reasonableness and Warrant Clauses*, 10 N.M. L. REV. 33, 35–41 (1979–1980) (providing a historical account of the origins and drafting of the Fourth Amendment).

[30] *Search (s. from the verb)*, JOHN ASH, THE NEW AND COMPLETE DICTIONARY OF THE ENGLISH LANGUAGE: TO WHICH IS PREFIXED, A COMPREHENSIVE GRAMMAR (2d ed. 1795).

[31] *Search*, OXFORD ENGLISH DICTIONARY (2d ed. 1989).

[32] *See, e.g.*, New York v. Class, 475 U.S. 106, 114 (1986) (holding that a police officer's opening of a car door to locate a vehicle identification number was not a search).

[33] *E.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (ruling that the text of the Fourth Amendment expressly limits its coverage to tangible items), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[34] *E.g.*, Silverman v. United States, 365 U.S. 505, 510–12 (1961) (discussing cases holding that the government did not commit a Fourth Amendment "search" when it did not encroach on any constitutionally protected area, such as a house or office).

[35] 277 U.S. at 456–57, 466.

[36] *Id.* at 457, 464.

This rigid conception of the Fourth Amendment allowed for widespread government wiretapping and bugging during the middle decades of the twentieth century. From 1941 to the mid-1960s, for instance, the FBI recorded nearly a half million conversations.[37] It often used these recordings to monitor political groups, influence judicial appointments, threaten civil rights leaders, and intimidate or discredit members of Congress investigating its activities.[38]

In 1967, the Supreme Court reversed course.[39] In *Katz v. United States*, the Court held that government agents conducted a search when they placed a recording device on the outside of a public telephone booth and recorded a telephone conversation.[40] The Court overturned *Olmstead* and rejected the idea that the Fourth Amendment was limited to certain areas or to tangible objects.[41] The majority opinion did not, however, set out any new method of discerning the Fourth Amendment's extent.[42] Nor did it explain the reasoning behind its holding in any detail, except to say that the telephone had come to play a "vital role" in private communication.[43]

The test that governs the Fourth Amendment's scope in most cases[44] comes instead from Justice Harlan's short concurrence in *Katz*. Harlan described the test's two requirements as follows: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[45] In subsequent cases, this is often stated as a single inquiry—whether the

---

[37] ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT 17 (1992); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 583 (2011).

[38] CHARNS, *supra* note 37, at 17, 24–31; Tokson, *supra* note 37, at 583.

[39] *See* Berger v. New York, 388 U.S. 41, 44, 54 (1967); Katz v. United States, 389 U.S. 347, 359 (1967). The Court may have been motivated by the growing controversy over FBI wiretapping practices and the Justice Department's increasing disclosure of such practices to the courts. *See* CHARNS, *supra* note 37, at 77; CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 593–94 (1991).

[40] 389 U.S. at 348, 353.

[41] *Id.* at 350–51, 353.

[42] *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385 (1974).

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

[44] Acts of government that trespass on constitutionally protected areas may also violate the Fourth Amendment. After decades of largely ignoring trespass concepts in Fourth Amendment law, the Supreme Court has recently decided two cases based on the finding that police officers committed a physical intrusion while seeking information. Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013); United States v. Jones, 132 S. Ct. 945, 950–51 (2012).

[45] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

person at issue had a reasonable expectation of privacy in the thing examined by the police.[46]

The *Katz* test is simple and concise on the page. But in application it is frequently puzzling, and its true nature remains something of a mystery.[47] Is it a probabilistic test, asking whether a person is empirically likely to be observed in a certain context? Or is it largely a normative test, asking whether a person should be entitled to expect privacy in certain aspects of life? Arguably, the test has both empirical and normative elements, but how these elements interact or how to reconcile them when they conflict remains unclear.[48]

B. From Subjective Expectation to Knowing Exposure

Adding to the confusion surrounding the *Katz* test is the Court's acknowledgement that the subjective portion of the test should not be applied literally.[49] If the scope of the Fourth Amendment actually depended upon the subjective beliefs of a citizen, then the government could insulate invasive surveillance programs from Fourth Amendment challenge simply by announcing them to people in advance. For example, a state could announce that it will henceforth conduct random searches of all houses owned by citizens with a prior drug conviction. Following the announcement, no citizen with a prior drug conviction would expect her house to be safe from government search. Yet the Court has said that it would not apply the subjective test in such a situation, and would instead find that citizens have a reasonable expectation of privacy in their homes despite the absence of a subjective expectation of privacy.[50]

---

[46] *E.g.*, New York v. Class, 475 U.S. 106, 112 (1986) (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring)) ("[T]he State's intrusion . . . cannot result in a Fourth Amendment violation unless the area is one in which there is a 'constitutionally protected reasonable expectation of privacy.'"); Oliver v. United States, 466 U.S. 170, 177 (1984) (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring)) ("Since *Katz v. United States*, the touchstone of Amendment analysis has been the question whether a person has a 'constitutionally protected reasonable expectation of privacy.'").

[47] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 533–34 (2011) ("[T]he 'reasonable expectation of privacy' test is widely considered one of the great mysteries of Fourth Amendment law . . . and opinions differ on even the basic question of whether the inquiry is descriptive or normative." (footnotes omitted)).

[48] This issue is discussed below in Part II and Section V.A.

[49] *See infra* note 50.

[50] Smith v. Maryland, 442 U.S. 735, 740–41 n.5 (1979); *see also* Hudson v. Palmer, 468 U.S. 517, 525 n.7 (1984) ("The Court has always emphasized" the objective reasonableness prong of the *Katz* test rather than "the privacy expectations of particular defendants in particular situations . . . ." (quoting United States v. White, 401 U.S. 745, 751 (1971) (plurality opinion)).

Moreover, courts apply the subjective prong of the *Katz* test in only a small minority of cases (roughly 12%, according to one study).[51] Even in those cases, the subjective prong rarely determines case outcomes.[52]

Courts appear to deemphasize an individual's subjective expectation and to focus instead on whether the individual has knowingly waived her privacy in her information (or her property, etc.) such that the Fourth Amendment no longer protects it.[53] If the person has knowingly exposed her information to the public, for instance by publishing it in a newspaper, then she no longer has a reasonable expectation of privacy in the information.[54] If she has not knowingly exposed her information, then the information is protected so long as people would generally consider it reasonable to expect privacy in the information.[55]

Thus, in practice, the *Katz* test seems to ask the following: (1) Has the person in question waived her privacy in her information by knowingly exposing it to the public? and (2) If not, then could the person have had an objectively reasonable expectation of privacy in the information? If there was no waiver and if the person could reasonably expect privacy, then the Fourth Amendment applies, and the police generally must obtain a warrant before examining the information at issue.

The analysis of knowledge plays a pivotal role in both parts of the *Katz* test. The next Section explores how courts use knowledge to determine "knowing exposure" to the public and to measure reasonable expectations of privacy.[56]

---

[51] Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 117–18 (2015) (examining every case that applied the *Katz* test in 2012 and finding that only 12% of Fourth Amendment cases decided that year purported to apply the subjective prong).

[52] *Id.* at 119–21.

[53] *Id.* at 128–29 (discussing the shifting of the Supreme Court's typical Fourth Amendment inquiry from subjective expectation to knowing exposure); *Smith*, 442 U.S. at 740–41 n.5 (directing courts to ignore the subjective prong in certain situations where it would dictate a different outcome than the objective prong); *see also infra* Section II.C (describing Fourth Amendment cases applying the knowing exposure test).

[54] *See* Kerr, *supra* note 51, at 126–27 (discussing voluntary exposure cases and describing the subjective test in these cases as "akin to a consent doctrine"). Several cases applying this principle are discussed in Section II.C.

[55] Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring).

[56] *See id.* at 351 (majority opinion) (citing Lewis v. United States, 385 U.S. 206, 210 (1966)) (holding that there is no Fourth Amendment protection for information that a person "knowingly exposes to the public").

II. KNOWLEDGE AND THE REASONABLE EXPECTATION OF PRIVACY

As mentioned above, the *Katz* inquiry into reasonable expectations of privacy can have both empirical and normative elements.[57] Courts sometimes engage in normative analysis when deciding Fourth Amendment cases.[58] On rare occasions, they rely exclusively on such an analysis.[59] But typically, courts applying *Katz* inquire into people's actual expectations of privacy.[60]

In these cases, the *Katz* inquiry frequently hinges on the assessment of what members of society know. Likewise, assertions about knowledge play a substantial role in cases that look to both expectations of privacy and normative considerations.[61] This Part examines how courts have used knowledge to help define the Fourth Amendment's boundaries.[62]

A. Knowledge and Expectation

As noted above, the concept of knowing exposure to the public plays a large role in determining the reach of the Fourth Amendment following *Katz*.[63] Assessing people's knowledge is, of course, essential to determining whether they have knowingly exposed their information to the public. But knowledge plays an even broader role in determining the Fourth Amendment's scope. What a person expects is largely a function of what they know. If I know that a high school band marches past my house every Sunday morning from 10:00 to 10:30 AM, then it is reasonable for me to expect a lot of noise on Sunday mornings. It is also reasonable to expect

---

[57] *See supra* text accompanying notes 47–48.

[58] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001).

[59] Hudson v. Palmer, 468 U.S. 517, 526–27 (1984); *see also* Illinois v. Caballes, 543 U.S. 405, 407–09 (2005) (holding that a dog sniff is not a Fourth Amendment search because any expectation of privacy in contraband cannot be "legitimate").

[60] *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000); Minnesota v. Olson, 495 U.S. 91, 98–99 (1990); California v. Greenwood, 486 U.S. 35, 40–41 (1988); United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007).

[61] *See, e.g.*, California v. Carney, 471 U.S. 386, 393–94 (1985); Smith v. Maryland, 442 U.S. 735, 742–45 (1979).

[62] This Article's analysis is limited to the assessment of expectations of privacy in Fourth Amendment law. Although courts examine expectations of privacy in privacy tort cases, the inquiry is different in several substantial ways. *See* Strahilevitz, *supra* note 19, at 933–34 & n.35 (noting, for example, that the objective inquiry predominates in Fourth Amendment law, while subjective expectations play a large role in privacy torts). Further, privacy tort cases have typically eschewed inquiry into societal expectations of privacy, focusing instead on the *ex ante* likelihood of public dissemination of the plaintiff's personal information. *Id.* at 934–35.

[63] *See* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 146–47 (2002) (discussing the importance of the "knowing exposure" concept in Fourth Amendment law).

that I will not have much privacy when I sunbathe in my front yard between 10:00 and 10:30 AM. My expectations of privacy stem from my knowledge about the band. In this scenario and countless others, knowledge is the foundation on which expectations are built.

Assessing knowledge can also provide courts with a way to make the complex *Katz* inquiry into "expectation" more tractable. An expectation is an internal belief about the uncertain future. Other people's expectations can be difficult to intuit, and there will rarely be direct external evidence of a person's expectations in a given situation. By contrast, a person's knowledge is more likely to be inferable from external sources, such as something she has seen or read.

Courts frequently rely on their assessments of knowledge to determine whether a person has a reasonable expectation of privacy.[64] But courts' examination of knowledge tends to be broad and abstract rather than particular. They generally look to what a person *should* know, rather than what she actually did know.[65] In the Fourth Amendment context, courts do this by reaching a conclusion about the collective knowledge possessed by society and then imputing that knowledge to the person at issue.[66] Thus, if most people know that taking an action would result in a loss of privacy, then an individual taking that action will be found to have "knowingly" exposed her information, regardless of her actual knowledge.[67] For example, in *United States v. Forrester*,[68] the Ninth Circuit held that a defendant had knowingly exposed his email to/from information and the IP addresses of the websites he visited. The court concluded that users in general "should know that this information is provided to and used by Internet service providers."[69] It did not inquire whether the defendant actually knew that he was exposing his data to third parties.[70]

It may seem strange for courts to decide that an individual has knowingly waived her privacy based not on what she knew but on what

---

[64] *See infra* Sections II.B–II.C.

[65] *See, e.g.*, City of Ontario v. Quon, 560 U.S. 746, 762 (2010) (reasoning that Quon "should have known" that his text messages would be read by his employers); *see* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 268 (2002) ("[T]he Court has indicated that government need not show actual knowledge of exposure to nullify Fourth Amendment protection. If a target *should have* known public exposure might occur, the Court has held, one assumes the risk of such exposure and loses Fourth Amendment protection.").

[66] *See infra* note 67.

[67] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (finding that a telephone user knowingly exposed the numbers that he dialed).

[68] 512 F.3d 500, 510 (9th Cir. 2007).

[69] *Id.*

[70] *See id.* at 509–10.

people in general know.[71] But there are several advantages to this method from the perspective of the courts. Basing the scope of the Fourth Amendment on what each individual knows about the disclosure of her information would substantially increase decision costs for judges and render the Fourth Amendment's coverage inconsistent across similar fact patterns. Judges addressing a common police surveillance situation could not simply decide the case based on prior case law but would have to engage in a fact-heavy assessment of each individual's state of knowledge. In many cases there would be no extrinsic evidence of the person's knowledge, and she would have strong incentives to feign ignorance or otherwise obscure her actual knowledge.[72] By contrast, if everyone is presumed to have a standard set of societal knowledge, then case outcomes will be the same for all parties.

Of course, it is possible that courts making assertions about societal knowledge may not actually be concerned with empirical accuracy. The rhetoric of knowledge may, for these courts, mask the normative judgment that actually drives the decision.[73] Such a possibility can neither be proved nor entirely ruled out. What is clear is that the concept and the language of societal knowledge play a prominent role in Fourth Amendment law, and many courts engage in detailed examinations of societal knowledge about privacy and surveillance.[74]

The next few Sections examine how courts have used assessments of societal knowledge to reach broad conclusions about the Fourth Amendment's scope.

---

[71] Overt consideration of societal knowledge is rare in the law, although there are a few areas of law that expressly evaluate it. In trademark dilution claims under 15 U.S.C. § 1125(c)(2)(A) (2012), courts assess whether the plaintiff's mark is "famous," defined as "widely recognized by the general consuming public of the United States." This inquiry essentially asks how aware the public is of a certain brand. *See, e.g.*, Coach Svcs., Inc. v. Triumph Learning LLC, 668 F.3d 1356, 1373–76 (Fed. Cir. 2012). Requests for change of venue often involve assertions about potential jurors' awareness of a relevant news story. *See* Williams v. Superior Court, 668 P.2d 799, 801–04 (Cal. 1983) (in bank). This inquiry is not society-wide, however, and is typically limited to one jurisdiction. *See id.*

[72] *See* Strahilevitz, *supra* note 19, at 933.

[73] *See* CYNTHIA LEE, MURDER AND THE REASONABLE MAN 240–42 (2003) (discussing the normative considerations driving some seemingly positivist Fourth Amendment decisions); Kerr, *supra* note 19, at 519, 522 (suggesting that normative considerations may drive outcomes in Fourth Amendment cases even when the opinion focuses on expectations of privacy or positive law); *see also infra* the discussion accompanying notes 346–49.

[74] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742–43 (1979); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 140 & n.19, 146 (E.D.N.Y. 2013); State v. Reid, 945 A.2d 26, 33 (N.J. 2008).

B. The Knowledge Inquiry in Reasonable Expectations of Privacy Cases

People's knowledge about surveillance technologies, police practices, existing laws, and the behavior of private entities shapes their expectations of privacy. Courts accordingly look to collective knowledge when attempting to determine which expectations of privacy are reasonable.

For example, government regulations can themselves erode people's expectations of privacy, as long as people are generally aware of the regulations. Vehicle owners' collective knowledge provides a basis for diminished Fourth Amendment protection for automobiles. The Supreme Court has concluded that "[t]he public is fully aware that it is accorded less privacy in its automobiles" because of the pervasive nature of automobile regulation and the "everyday occurrence" of police stops for minor infractions.[75] As a result, "there is a reduced expectation of privacy" in motor vehicles.[76]

The Court has found that participants in certain heavily regulated businesses lack a reasonable expectation of privacy in their business records and property because they "must already be aware" of a history of close government supervision over such businesses.[77] Under this reasoning, the Fourth Amendment does not cover most government inspections of liquor stores,[78] firearms dealerships,[79] mining facilities,[80] or junkyards,[81] because when a person chooses to operate one of these businesses, she does so "with the knowledge" that her business records and property may be inspected.[82]

Similarly, in *City of Ontario v. Quon*, the Court held that a police officer had a limited expectation of privacy in the texts he sent from a city-

---

[75] California v. Carney, 471 U.S. 386, 392 (1985) (citation omitted); *see also* United States v. Ross, 456 U.S. 798, 806 n.8 (1982) (finding that "individuals always had been on notice that movable vessels may be stopped and searched on facts giving rise to probable cause that the vehicle contains contraband, without the protection afforded by a magistrate's prior evaluation of those facts").

[76] *Carney*, 471 U.S. at 393. This lowered expectation of privacy helps to justify the lack of a warrant requirement for automobile searches, so long as the police possess probable cause to search the automobile for evidence of a crime. *Id.* at 392.

[77] Marshall v. Barlow's, Inc., 436 U.S. 307, 313 (1978).

[78] Colonnade Catering Corp. v. United States, 397 U.S. 72, 75–77 (1970).

[79] United States v. Biswell, 406 U.S. 311, 316 (1972).

[80] Donovan v. Dewey, 452 U.S. 594, 600, 602 (1981).

[81] New York v. Burger, 482 U.S. 691, 703–04 (1987).

[82] *Biswell*, 406 U.S. at 316; *see also, e.g.*, *Donovan*, 452 U.S. at 600 (finding no reasonable expectation of privacy when "the federal regulatory presence is sufficiently comprehensive and defined that the owner of commercial property cannot help but be aware that his property will be subject to periodic inspections undertaken for specific purposes").

owned pager because he should have known that the texts might be read.[83] Although the officer's supervisor had told him that the department would not audit his messages due to data overages, the Court nonetheless concluded that a reasonable officer "would or should have known that his actions were likely to come under legal scrutiny" at some point, and that "a reasonable employee would be aware" that his pager would eventually be audited.[84]

Just as knowledge can undermine privacy, lack of knowledge can be the basis for upholding it. For example, the Court held that a seller maintained a reasonable expectation of privacy in pornographic videos shipped in a package that was opened by a private party and then sent to the FBI.[85] The fact that the package was opened during shipping did not affect the seller's Fourth Amendment rights, because the seller had no way of knowing about it and no reason to expect it.[86] People's expectations of privacy could not be "altered in any way by subsequent events of which they were obviously unaware."[87]

Even when the Court's assessment of societal knowledge is largely implicit, it is often an important issue in Fourth Amendment cases. Dissenting Justices sometimes argue that the majority has incorrectly assessed collective knowledge and accordingly reached an erroneous conclusion about expectations of privacy. For instance, in *Bond v. United States*,[88] Justice Breyer (joined in dissent by Justice Scalia) argued that there was no general expectation of privacy against police touching of carry-on luggage because "[a]ny person who has travelled on a common carrier knows that luggage placed in an overhead compartment is always at the mercy of all people who want to rearrange or move previously placed luggage."[89] The dissenters disagreed with the majority's implicit determination that bus passengers were unaware that their luggage was

---

[83] City of Ontario v. Quon, 560 U.S. 746, 762 (2010).

[84] *Id.* at 752, 762; *see also id.* at 766 (Stevens, J., concurring) ("[I]t is clear that respondent Jeff Quon, as a law enforcement officer who served on a SWAT Team, should have understood that all of his work-related actions—including all of his communications on his official pager—were likely to be subject to public and legal scrutiny.").

[85] Walter v. United States, 447 U.S. 649, 658–59 (1980) (opinion of Stevens, J.).

[86] *Id.* at 658–59 & n.12.

[87] *Id.* at 658–59 n.12.

[88] 529 U.S. 334 (2000).

[89] *Id.* at 340 (Breyer, J., dissenting) (quoting United States v. McDonald, 100 F.3d 1320, 1327 (7th Cir. 1996), *abrogated by Bond*, 529 U.S. 334); *see also* California v. Ciraolo, 476 U.S. 207, 223–24 & n.8 (1986) (Powell, J., dissenting) (contending that people know that there is little risk of overflight surveillance from commercial aircraft).

likely to be handled or probed. As a result, they disagreed on the ultimate question of whether passengers had an expectation of privacy.[90]

The use of collective knowledge to set the boundaries of Fourth Amendment protection is not confined to the Supreme Court. Lower courts and state courts have also relied heavily on assessments of knowledge when determining reasonable expectations of privacy under the *Katz* test. For example, knowledge of workplace policies or inspection protocols can defeat a reasonable expectation of privacy in one's office[91] or on one's hard drive.[92] Parolees' awareness of the possibility of intrusions into their houses by parole officers results in "a severely diminished expectation of privacy" in their homes.[93] Prisoners' knowledge of mail inspection policies can eliminate any expectation of privacy in their letters.[94] And, although mine owners "cannot help but be aware that [they] 'will be subject to effective inspection'" and thus lack a Fourth Amendment right against warrantless inspections, mine employees are not "on notice" that they personally will be examined and therefore retain Fourth Amendment protection against personal searches.[95] Courts recognize that people's expectations of privacy are largely a function of what they know, and, accordingly, courts frequently assess societal knowledge in Fourth Amendment cases.

C. The Knowledge Inquiry in "Knowing Exposure" Cases

Societal knowledge also plays a prominent role in cases where the government asserts that an individual has "knowingly expose[d]" her information to the public and thereby waived any claim to Fourth Amendment protection.[96] If a person knows or should know that others can easily access their information, but takes no steps to prevent such access, then courts are likely to find that she lacks any reasonable expectation of

---

[90] *See Bond*, 529 U.S. at 339–40 (Breyer, J., dissenting).

[91] *See, e.g.*, Schowengerdt v. United States, 944 F.2d 483, 488 (9th Cir. 1991).

[92] *See, e.g.*, Bradley v. Pfizer, Inc., 440 F. App'x 805, 810 (11th Cir. 2011).

[93] United States v. Newton, 369 F.3d 659, 665 (2d Cir. 2004) (quoting United States v. Reyes, 283 F.3d 446, 461 (2d Cir. 2002)); *see also, e.g.*, United States v. Hedrick, 146 F. App'x 871, 872 (9th Cir. 2005) ("Since the inception of the probation and parole systems, probationers and parolees have understood that they are subject to home visits from time to time . . . ."); United States v. Wilson, 105 F. App'x 498, 500 (4th Cir. 2004) (per curiam) (finding the defendant "was aware that his expectation of privacy was diminished by virtue of his parolee status"); State v. Patrick, 381 So. 2d 501, 503 (La. 1980) (finding that "defendant was aware that he would be searched upon his re-entry into the detention facility at the end of each day" and thus his "expectations of privacy were minimal, if any, under the circumstances").

[94] *See, e.g.*, State v. Wiley, 565 S.E.2d 22, 33 (N.C. 2002).

[95] Commonwealth v. Burgan, 450 S.E.2d 177, 180 (Va. Ct. App. 1994) (quoting Donovan v. Dewey, 452 U.S. 594, 603 (1981)).

[96] Katz v. United States, 389 U.S. 347, 351 (1967).

privacy. This concept has become increasingly important due to the expanding role of the "third party doctrine," which holds that the Fourth Amendment does not apply to personal information disclosed to a party other than the intended recipient of a communication.[97] Thus, knowing exposure can eliminate Fourth Amendment protection when information is exposed to the whole world[98] or just a single third party.[99]

Courts typically determine whether a person has knowingly exposed her information by assessing what people in general know about information exposure and then attributing that knowledge to the individual. For example, the Court analyzed public knowledge in *Smith v. Maryland*, ruling that Fourth Amendment protection does not extend to dialed telephone numbers.[100] The Court explained that telephone users knowingly disclose telephone numbers to a third party and thereby waive their privacy:

> 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.[101]

The Court also emphasized that most telephone books contain a page labeled "Consumer Information" that informs readers that the telephone company "can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls."[102] The Court concluded that telephone

---

[97] For an example of the Court applying third-party doctrine, see *Smith v. Maryland*, 442 U.S. 735, 744–45 (1979). The third-party doctrine's significance in Fourth Amendment law has increased in the internet age, as an ever-growing amount of information is transmitted or stored by third-party service providers. *See* Tokson, *supra* note 37, at 598, 602–04.

[98] *E.g.*, California v. Ciraolo, 476 U.S. 207, 213–14 (1986).

[99] *E.g.*, *Smith*, 442 U.S. at 744–45 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)); Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no Fourth Amendment protection when an informant "was in the suite by invitation, and every conversation which he heard was either directed to him or knowingly carried on in his presence").

[100] *Smith*, 442 U.S. at 745–46. Accordingly, the police may capture such numbers with an electronic device, even in the absence of a warrant or any suspicion. *Id.*

[101] *Id.* at 742. The Court then discussed how "pen registers"—electronic devices used for recording dialed telephone numbers—were used in fraud investigations and where a phone is subject to a special billing structure. *Id.* (citing United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977)); Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 266 (9th Cir. 1977)). Although the Court conceded that "most people may be oblivious" to these specific uses of pen registers, "they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls." *Id.* (citing Von Lusch v. C & P Tel. Co., 457 F. Supp. 814, 816 (D. Md. 1978)).

[102] *Id.* at 742–43 (first citing BALTIMORE TELEPHONE DIRECTORY 21 (1978); and then citing DISTRICT OF COLUMBIA TELEPHONE DIRECTORY 13 (1978)).

users "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."[103] As a result, the Court held that no rational telephone subscriber could expect her dialed telephone numbers to be private.[104]

Similarly, the Supreme Court found knowing exposure to the public in *California v. Greenwood*,[105] holding that the police can open and examine the contents of trash bags left on the curb outside of a house without conducting any "search" under the Fourth Amendment.[106] The Court found that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[107] Accordingly, the defendants could have no reasonable expectation of privacy in the garbage that they knowingly exposed to potential "public inspection."[108]

State courts and lower courts likewise frequently assess societal knowledge when analyzing whether a person has knowingly exposed her information to the public. In these cases, "public awareness" of third party data gathering can "negate any constitutionally sufficient expectation of privacy."[109] In recent years, these courts have relied upon assessments of collective knowledge to determine whether the Fourth Amendment applies to new technologies and contexts. Some of these cases draw direct analogies to the Supreme Court's cases relying on societal knowledge. For example, in *United States v. Forrester*,[110] the Ninth Circuit answered the question of whether the Fourth Amendment protects email to/from addresses and the IP addresses[111] of websites a user visits by drawing a parallel to the Court's assessment of collective knowledge in *Smith*.[112] The Ninth Circuit noted that "*Smith* based its holding that telephone users have

---

[103] *Id.* at 743.

[104] *Id.*

[105] 486 U.S. 35 (1988).

[106] *Id.* at 37.

[107] *Id.* at 40 (footnotes omitted) (citing People v. Krivda, 486 P.2d 1262, 1269 (Cal. 1971)).

[108] *Id.* at 41 (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981)).

[109] Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 256–57 (9th Cir. 1977) (footnote omitted); *see also* United States v. Clegg, 509 F.2d 605, 610 (5th Cir. 1975) ("[T]elephone subscribers have no reasonable expectation that records of their calls will not be made. It is, in fact, well known that such records are kept.").

[110] 512 F.3d 500 (9th Cir. 2008).

[111] In this context, an IP address is the unique sequence of numbers that identifies a website or group of websites on the internet. *See id.* at 510 n.5.

[112] *Id.* at 510.

no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment."[113] It then held that website and email addresses are not protected by the Fourth Amendment because of the knowledge of internet users: "users have no expectation of privacy . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[114] Other courts have held that users have a reasonable expectation of privacy in their IP address, based on their lack of knowledge about the internet: "[W]hen users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit."[115] Users' lack of understanding of how websites operate provided the basis for a reasonable expectation of privacy.[116]

Knowledge is also a key factor in deciding the Fourth Amendment status of other types of information, from the personal information associated with an Internet Service Provider (ISP) account,[117] to communications from a personal computer on a college's computer network.[118] In the first set of cases to address whether government collection of emails is covered by the Fourth Amendment, the Sixth Circuit held that the question depends on the knowledge of email users.[119] The

---

[113] *Id.*

[114] *Id.*

[115] State v. Reid, 945 A.2d 26, 33 (N.J. 2008). The court also stated that "[m]ore sophisticated users understand that [their IP addresses], standing alone, reveal[] little if anything to the outside world." *Id.* For these users, the knowledge that their IP addresses alone do not reveal their identities is the basis for a reasonable expectation of privacy in their IP addresses. *Id.* Apparently combining the knowledge of these sophisticated users with the lack of knowledge of most users, the court found a general reasonable expectation of privacy in a user's IP address. *Id.* Again, general societal knowledge was the touchstone of expectations of privacy.

[116] *Id.*

[117] *E.g.*, United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *3–4 (4th Cir. Aug. 3, 2000) (per curiam) (holding that a defendant's information was not protected by the Fourth Amendment because, when the defendant "entered into a service agreement with MindSpring, he knowingly revealed [his subscriber] information to MindSpring and its employees"); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005) (finding no expectation of privacy in subscriber information given to AOL because AOL customer agreement stated that AOL would turn over such information to the government if compelled by legal process).

[118] United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) (citing United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002)) ("[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user.").

[119] *See* Warshak v. United States (*Warshak I*), 490 F.3d 455, 473 (6th Cir. 2007), *vacated en banc on ripeness grounds*, Warshak v. United States (*Warshak II*), 532 F.3d 521, 523 (6th Cir. 2008); *Warshak II*, 532 F.3d at 526–27; Warshak v. United States (*Warshak III*), 631 F.3d 266, 287 (6th Cir. 2010).

judges inferred customers' knowledge based on the user agreements that their email service providers promulgate.[120] Thus, "where a user agreement explicitly provides that e-mails and other files will be monitored or audited . . . the user's knowledge of this fact may well extinguish his reasonable expectation of privacy."[121] The Sixth Circuit noted that the Fourth Amendment inquiry "may well shift over time" and would "assuredly shift[] from internet-service agreement to internet-service agreement."[122] It ultimately concluded that the defendant had a reasonable expectation of privacy in his emails because his ISP user agreement did not inform him that the ISP would "'audit, inspect, and monitor' its subscriber's emails."[123]

D. Knowledge in Fourth Amendment Scholarship

Much of the scholarship on the Fourth Amendment's scope assumes that courts must assess collective knowledge in applying *Katz*'s reasonable expectation of privacy test.[124] Several scholars have implicitly or explicitly endorsed this knowledge-centered approach.[125]

Mary Leary, for example, has written that courts should be especially attentive to consumer knowledge when answering Fourth Amendment questions.[126] She contends that a consumer does not waive her right to privacy when a third party obtains information without the consumer's knowledge.[127] By contrast, the reduction of Fourth Amendment protection "seems fair to the consumer regarding information the consumer directly disclosed knowingly to the primary party."[128] Likewise, Orin Kerr has defended the Third Party Doctrine as a doctrine of knowing consent to a search, arguing that a person's disclosure of information constitutes consent to a search if and only if "[the] person knows that they are disclosing information to a third party."[129] Other scholars have made similar

---

[120] *See* cases cited *supra* note 119.

[121] *Warshak I*, 490 F.3d at 473.

[122] *Warshak II*, 532 F.3d at 526–27.

[123] *Warshak III*, 631 F.3d at 287.

[124] *See, e.g.*, Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1417–18 (2002).

[125] *See, e.g.*, Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 745 (2011); Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 549, 590, 592 (2013).

[126] Leary, *supra* note 5, at 378–80.

[127] *See id.* at 343.

[128] *Id.* at 380.

[129] Kerr, *supra* note 5, at 588.

arguments. Because knowledge provides the basis for people's reasonable expectations of privacy, assessments of knowledge pervade the scholarship of the *Katz* test no less than the cases applying it.[130]

E. Knowledge and New Surveillance Technologies—A Case Study

As government surveillance techniques evolve, they can pose novel and difficult Fourth Amendment questions. In the absence of controlling precedent, courts generally answer these questions by applying the *Katz* test. Courts examine people's reasonable expectations of privacy, and this inquiry naturally leads them to examine societal knowledge.[131] Yet assessing such knowledge is especially difficult in the context of new technologies and social practices. There are typically no surveys or other empirical studies to guide the inquiry and no long-established social practices to which judges can refer.[132]

This Section addresses one particularly important, and especially troubling, example of courts relying on societal knowledge to determine how the Fourth Amendment applies to new surveillance technologies. In recent years, law enforcement officials have frequently sought to track cell phone users by obtaining location data produced by the users' phones.[133] The resulting criminal cases are potentially of enormous importance in Fourth Amendment law. In these cases, courts are asked to reconcile two competing principles of Fourth Amendment jurisprudence. One is the recognition by five Justices of the Supreme Court that long-term surveillance of people's locations can be destructive of personal privacy.[134] The other is the Third Party Doctrine principle that information knowingly turned over to a third party cannot be protected by the Fourth Amendment.[135]

---

[130] *See, e.g.*, sources cited *supra* note 125; Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1327–28 (2012); Slobogin, *supra* note 124, at 1416–17.

[131] *See supra* Section II.A.

[132] By contrast, it may be easier to infer societal knowledge about practices such as trash collection, which had been around for decades by the time *California v. Greenwood* was decided. *See* 486 U.S. 35, 40 & nn.2–4 (1988); JON ROBERTS, OKLAHOMA DEP'T OF ENVTL. QUALITY, A BRIEF HISTORY OF WASTE REGULATION IN THE UNITED STATES AND OKLAHOMA, http://www.deq.state.ok.us/lpdnew/wastehistory/wastehistory.htm [https://perma.cc/V234-FDZL].

[133] *See* James Beck et al., *The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location—Part II*, 49 CRIM. L. BULL. 637 (2013).

[134] *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment) (contending that extended surveillance of a person's movements in public violates a reasonable expectation of privacy); *id.* at 955 (Sotomayor, J., concurring) (agreeing with Justice Alito and describing how locational surveillance "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").

[135] *See supra* notes 97–99 and accompanying text.

The federal appeals courts that have addressed the question of cell phone location tracking have resolved this tension by focusing intently on the collective knowledge of cell phone users.[136] This Section describes how cell phone location tracking works and examines how courts have used societal knowledge to address the difficult Fourth Amendment questions raised by this new form of surveillance.

1. Cell Site Location Information.—When you call a friend on your cell phone, the phone converts your voice into a signal that is transmitted via radio waves to a cell phone tower.[137] The cell phone tower system then relays the radio waves to your friend's phone, which translates them back into sound.[138]

When you place the call, your phone selects the cell site (i.e., the cell tower) with which it has the strongest connection; this is usually the closest tower.[139] Typically, different antennas on the tower will serve different sectors of the area around the tower.[140] By noting which antenna received your signal, the cell phone company can determine that you were in the particular sector covered by the antenna.[141] As the number of cell towers proliferates, this information can reveal your location within a relatively small geographic area.[142] Furthermore, federal law requires that cell phone companies maintain the capability to record a subject's cell site location information (CSLI) at the beginning and end of a call,[143] and cell phone companies do in fact record and store this location data for billing and other purposes.[144]

---

[136] *See infra* Section II.E.2.

[137] *E.g.*, Rong Wang, *How Do Cell Phones Work?*, PONG (Dec. 20, 2014), http://www.pongcase.com/blog/cell-phones-work/#sthash.GbY9H02y.73BMK76t.dpbs [https://perma.cc/MWZ8-YG82].

[138] *Id.*

[139] Beck et al., *supra* note 133, at 643. When a person makes a call, the phone connects to "the cell site with which it has the strongest connection," but "[d]ue to a number of factors, including topography and call volume, that tower is not always the *closest* tower to the cell phone." *Id.*

[140] *Id.* at 641.

[141] *Id.* at 645.

[142] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of H. Comm. on the Judiciary*, 111th Cong. 15–16 (2010) (testimony of Matt Blaze, Associate Professor, Penn Engineering) [hereinafter Blaze Testimony]. In addition, by recording the times that a user's telephone signal arrives at multiple cell towers, a company can calculate the phone's location with a precision similar to that of GPS. *Id.* at 23; *see* Beck et al., *supra* note 133, at 648.

[143] Communications Assistance for Law Enforcement Act, 14 FCC Rcd. 16794 ¶¶44–45 (1999) ("Third Report and Order"); Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002(a)(2) (2012).

[144] Beck et al., *supra* note 133, at 640.

Cell phone users can be tracked even when they are not making phone calls. An active cell phone "registers" with cell towers by emitting a signal roughly every seven seconds.[145] This allows the network to locate the phone so that it can receive and make calls.[146] It also allows cell phone companies to track users' locations constantly and accurately, by recording the times when a given cell phone's registration signal hits various cell towers.[147] Several cell companies store this highly precise location data along with similar data associated with incoming and outgoing calls.[148] This practice is likely widespread, because the relative cost of data storage is low and location data is useful for network management, research, and marketing.[149] However, the precise data retention policies of specific cellular providers tend to be unknown, as companies typically refuse to disclose such policies and may consider them to be trade secrets.[150]

2. Collective Knowledge in Location Surveillance Cases.—Like GPS location-tracking technology, CSLI can reveal intimate details about a person's life by allowing an observer to track wherever a person travels with her cell phone. As the D.C. Circuit has noted, someone "who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband . . . an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[151] Yet CSLI information is also transmitted to a third party and stored by that party in the ordinary course of business.[152]

Does the Fourth Amendment apply to this information? Courts have answered this complex question by examining the collective knowledge of

---

[145] *Id.* at 642. A cell phone in "airplane mode" does not communicate with cell towers. *Id.* at 642–43.

[146] *Id.*

[147] Blaze Testimony, *supra* note 142, at 27. Cell companies can also track users in real time via "pinging," the sending of a signal to a cell phone requesting its coordinates. *See* L. Scott Harrell, *Locating Mobile Phones Through Pinging and Triangulation*, PURSUIT MAG. (July 1, 2008), http://pursuitmag.com/locating-mobile-phones-through-pinging-and-triangulation [https://perma.cc/E8S9-LF2G].

[148] Blaze Testimony, *supra* note 142, at 27; Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1.

[149] Blaze Testimony, *supra* note 142, at 27–28.

[150] Freiwald, *supra* note 125, at 719; *see also* Suzanne Choney, *How Long Do Wireless Carriers Keep Your Data?*, NBC NEWS (Sep. 29, 2011, 3:05 PM), http://www.nbcnews.com/tech/mobile/how-long-do-wireless-carriers-keep-your-data-f120367 [https://perma.cc/GM5H-6QHT] (describing an ACLU FOIA request that revealed general policies on cell tower records but no details on the accuracy of information stored).

[151] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

[152] *See supra* notes 141–44 and accompanying text.

cell phone users regarding their locational privacy.[153] For example, in each of the federal appellate cases that have squarely faced the issue, collective knowledge has been a decisive factor in determining the extent of Fourth Amendment protection.[154]

The Third Circuit held that a cell phone user had not waived his privacy in his CSLI, because "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."[155] The court reasoned that "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller."[156]

Using collective knowledge as the dispositive factor, the Fifth Circuit reached the opposite conclusion. It ruled that "users know that they convey information about their location to their service providers when they make a call and . . . they voluntarily continue to make such calls," thereby forfeiting any expectation of privacy.[157] The court reasoned that cell phone

---

[153] *See, e.g.*, *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(c)–(d), 42 F. Supp. 3d 511, 518 (S.D.N.Y. 2014) ("[S]ubscribers are aware that use of their cell phones necessitates disclosure of the information sought."); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y. 2013) (citing *In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011)) ("[I]t is clearly within the knowledge of cell phone users that their telecommunication carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time."); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012) (It is "common knowledge that communications companies regularly collect and maintain all types of non-content information regarding cell-phone communications, including cell-site tower data, for cell phones for which they provide service."); United States v. Graham, 846 F. Supp. 2d 384, 401 (D. Md. 2012) ("[A]ny assumption of ignorance is belied by Sprint/Nextel, Inc.'s privacy policy, which informs its customers that it collects location data." (footnote omitted)); *see also* Freiwald, *supra* note 125, at 733–37.

[154] The Sixth Circuit has ruled that police pursuing a person engaged in the transportation of drugs may track the transporter's cell phone without triggering the Fourth Amendment. The court relied on a previous Supreme Court case involving the use of a tracking beeper to aid visual surveillance and did not find it necessary to address knowledge. United States v. Skinner, 690 F.3d 772, 777–78 (6th Cir. 2012) (citing United States v. Knotts, 460 U.S. 276 (1983)); United States v. Forest, 355 F.3d 942, 950–51 (6th Cir. 2004). Knowledge plays a prominent role in the Sixth Circuit's most recent case addressing cell phone location information, *United States v. Carpenter*, 819 F.3d 880, 887–88 (6th Cir. 2016).

[155] *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Svc. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010).

[156] *Id.* (alteration in original) (quoting Brief for Electronic Frontier Foundation et al. as Amici Curiae in Support of Affirmance of the District Court at 21, *In re* Order Directing Elec. Commc'n Svc. To Disclose Records, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866619).

[157] *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013). The court made additional, related findings, stating that:

> A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call. . . . Cell phone users recognize that, if their phone cannot pick up a signal (or "has no bars"), they are out of the range of their service provider's network of towers. And they realize that, if many customers in an

companies' terms of service and privacy policies "inform subscribers that the providers not only use [CSLI] information, but collect it."[158] The Sixth Circuit has similarly concluded that "any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."[159] The Fourth Circuit has likewise held that people know they are conveying their location data to their cell phone company and therefore have no Fourth Amendment right in such data.[160] And the Eleventh Circuit has also denied Fourth Amendment protection for CSLI, determining that cell phone users "know . . . that cell phone companies make records of [their] cell-tower usage."[161] The court found that there were sufficient "publicly available facts" regarding CSLI that cell phone users could have no reasonable expectation of privacy in their location data.[162]

In these cases and countless others, courts' assessments of societal knowledge have played a central role in determining whether the Fourth Amendment applies to new technologies and social contexts. This trend is likely to continue, or even to accelerate, as technological change increasingly confronts courts with novel Fourth Amendment questions.

---

area attempt to make calls at the same time, they may overload the network's local towers, and the calls may not go through.

Id. at 613 (citing *Madison*, 2012 WL 3095357, at *8).

[158] *Id.* (citing *Madison*, 2012 WL 3095357, at *8).

[159] *Carpenter*, 819 F.3d at 888 (citing United States v. Davis (*Davis II*), 785 F.3d 498, 511 (11th Cir. 2015) (en banc)). The court also found that "any cellphone user who has paid 'roaming' (i.e., out-of-network) charges—or even cellphone users who have not—should know that wireless carriers have 'facilities for recording' locational information and that 'the phone company does in fact record this information for a variety of legitimate business purposes.'" *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979)).

[160] United States v. Graham (*Graham II*), No. 12-4659, 2016 WL 3068018, at *5 (4th Cir. May 31, 2016) (en banc). This decision reversed a prior panel decision that had reached the opposite conclusion about cell users' knowledge, finding "no reason to suppose that users generally know what cell sites transmit their communications or where those cell sites are located." United States v. Graham (*Graham I*), 796 F.3d 332, 356 (4th Cir. 2015), *aff'd in part on reh'g en banc*, 2016 WL 3068018 (May 31, 2016).

[161] *Davis II*, 785 F.3d at 511. This decision reversed a prior panel decision that came to the opposite conclusion about cell users' knowledge, holding that cell phone users do not knowingly disclose their location information to cell phone providers and therefore maintain a reasonable expectation of privacy in their CSLI. United States v. Davis (*Davis I*), 754 F.3d 1205, 1217 (11th Cir. 2014), *aff'd in part, vacated in part on reh'g en banc*, 785 F.3d 498 (2015).

[162] *Davis II*, 785 F.3d at 511 (citing *Smith*, 442 U.S. at 742–43).

III. CONCEPTUAL AND PRACTICAL PROBLEMS OF FOURTH AMENDMENT SOCIETAL KNOWLEDGE

As shown in Part II, courts frequently rely on societal knowledge to determine the Fourth Amendment's scope. Indeed, examining such knowledge is an important part of determining whether people have a reasonable expectation of privacy in their personal information or whether they have "knowingly exposed" information to another. However, as this Part details, there are fundamental conceptual and practical problems inherent in the assessment of Fourth Amendment societal knowledge.

A. Conceptual Problems

Attempting to determine what society "knows" about something presents several complex conceptual problems. Some of these arise because the concept of societal knowledge is itself so difficult to define, let alone measure. Others stem from the fact that the populace may rationally limit its awareness of even basic information about technology and public policy. This section discusses some of the serious conceptual flaws in courts' assessments of societal knowledge.

1. The Phases of Knowledge.—Knowledge is not a binary, all-or-nothing concept. There are many layers between being completely ignorant of a fact or idea and possessing the detailed understanding of an expert in the field. Societal knowledge is even more complex. At any given time, different members of society will have different levels of knowledge of a particular idea. Some citizens will be completely unaware of the idea, some will have a vague familiarity with it, some will comprehend it at a superficial level, and some will possess a deep understanding of the idea, its context, and its uses. Which of these groups of people have "knowledge" of the information in the relevant sense? Although it has not been recognized by courts or the Fourth Amendment literature, the complexity of knowledge has been discussed in a variety of other areas of social science. It has received particular attention in studies on the diffusion of innovations and in information and marketing theory. Research in these areas has identified several different stages of knowledge.[163]

[163] Similar stages of knowledge are recognized in the social science literature on marketing, advertising, and communications. Numerous models of the effects of marketing identify a multistage process of acquiring knowledge of a product that encompasses exposure, awareness, perception, comprehension, and integration with existing knowledge, among other steps. *See, e.g.*, Thomas E. Barry, *The Development of the Hierarchy of Effects: An Historical Perspective*, 10 CURRENT ISSUES & RES. ADVERT. 251, 263–66 (1987) (reviewing studies tracking consumers' purchasing and decisionmaking habits, measuring the effectiveness of advertisements, and considering the tension between buyers' beliefs and behavior).

At the most basic level is an *awareness* of some idea or thing, for instance a new product.[164] An individual at this stage has heard of the new product. If asked, she may recall that it exists, but she lacks details concerning it. She may know only its name but not what the "product is, what it will do, or how it will work."[165] For example, an individual in 2005 might see a news report on Facebook, but may not know what it does or even what a social network is.

A second stage is *basic comprehension*.[166] An individual with basic comprehension of a thing would generally know how it works, its basic purpose, and the likely consequences of using it.[167] For instance, an individual in 2007 might know how people generally use Facebook and what a social network is. She is far from an expert and lacks some important details, but she understands the overall concept of Facebook.

The final, deepest stage is comprehending a thing's *underlying principles*.[168] In general terms, this would mean understanding the theory behind something, knowing why it was developed and why people use it, grasping its larger meaning, and integrating it with one's overall understanding of the world.[169] An individual in 2009, for instance, could develop a relatively sophisticated understanding of how Facebook is designed and how people use it. She might appreciate how people use Facebook to develop and reinforce social connections, or the strategic ways that people present themselves in their profiles, or how Facebook's features are designed to promote deeper engagement and the sharing of detailed personal data.

Because knowledge is complex and multilayered, it can be difficult to ascertain how much people actually know about a given idea or fact. Nor is it clear which level of knowledge should be required before someone is deemed to "knowingly expose" their information or to lack a reasonable expectation of privacy.[170] Most likely, different levels of knowledge should

---

[164] EVERETT M. ROGERS, DIFFUSION OF INNOVATIONS 172–73 (5th ed. 2003).

[165] GEORGE M. BEAL & JOE M. BOHLEN, IOWA COOP. EXTENSION SERV., IOWA STATE UNIV. OF SCI. AND TECH., THE DIFFUSION PROCESS, SPECIAL REPORT NO. 18, at 2 (1981), http://www.soc.iastate.edu/extension/pub/comm/SP18.pdf [https://perma.cc/HEJ3-X5PL] (reprint of an influential early field report on the diffusion of innovations).

[166] *See* ROGERS, *supra* note 164, at 173, 199.

[167] *Id.* at 173.

[168] *Id.*

[169] *Id.*

[170] *See* Katz v. United States, 389 U.S. 347, 351 (1967) (citing Lewis v. United States, 385 U.S. 206, 210 (1966)) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *id.* at 361–62 (Harlan, J., concurring) (discussing "reasonable expectations of privacy").

be required in different factual contexts, with a detailed understanding of underlying principles necessary in cases where the privacy implications of people's actions are nuanced or complex, while in other cases basic comprehension would suffice. Instead, courts' failures to appreciate the multilevel nature of knowledge often lead them to find knowing waiver of Fourth Amendment rights on the basis of vague awareness of complex ideas.[171]

These difficulties are compounded when the inquiry calls for assessing societal knowledge, a fluid and dynamic phenomenon. Individuals move through the different phases of knowledge in different ways. Some will progress quickly to a deep understanding, others will learn slowly, and some will never achieve even basic comprehension of a new thing.[172] This makes societal knowledge complex and unstable, and it can also lead to fairness and distributional issues, as Section III.A.4 describes. Moreover, as the next Section discusses, some people who are exposed to information about a thing will nonetheless fail to become aware of it, let alone understand it in depth.

2. Selective Perception.—Although a great deal of information may be available about things like surveillance technologies, police practices, and existing laws, people may be predisposed to avoid such information where possible. People tend to seek out information that accords with their existing attitudes.[173] And, consciously or unconsciously, they tend to avoid information that conflicts with their existing beliefs.[174]

Of course, people may be exposed to information that they do not seek as passive consumers of televised or electronic information, or they may encounter information accidentally while seeking something else. Yet even in these cases, the phenomenon of *selective perception* may prevent them from becoming aware of the information.[175] Selective perception refers to people's failure to notice information that causes them emotional

---

[171] *See* discussion *supra* Section III.B.1.

[172] Beal & Bohlen, *supra* note 165, at 4–6 & fig.1; ROGERS, *supra* note 164, at 267, 282–89.

[173] ROGERS, *supra* note 164, at 171 (describing "the tendency to interpret communication messages in terms of the individual's existing attitudes and beliefs"); Matthew Tokson, *Judicial Resistance and Legal Change*, 82 U. CHI. L. REV. 901, 917 (2015) (discussing "the human tendency to seek out information that confirms (rather than contradicts) a given hypothesis").

[174] ROGERS, *supra* note 164, at 171 (describing the phenomenon of "selective exposure," where individuals "consciously or unconsciously avoid messages that are in conflict with their existing predispositions"); Raymond S. Nickerson, *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, 2 REV. GEN. PSYCHOL. 175, 176–78 (1998) (exploring the "widely recognized" phenomenon of people "tend[ing] not to seek and perhaps even to avoid information that would be considered counterindicative with respect to [favored] hypotheses or beliefs").

[175] RICKY W. GRIFFIN, FUNDAMENTALS OF MANAGEMENT 272 (8th ed. 2016).

discomfort or contradicts their prior beliefs.[176] If a boss views his favorite employee slacking off, for example, he may fail to consciously process what he sees. Conversely, if he sees a disliked employee doing the same thing, he is more likely to notice the behavior and remember it later.[177]

The lesson of selective perception is that one cannot tell what people are aware of even if one knows what they have seen or heard. Even non-disturbing news may escape people's attention. For example, people may fail to perceive information if they are distracted at the time of exposure or if they sense that the information is not relevant.[178] Selective perception may be especially relevant in the Fourth Amendment context because it can prevent people from becoming aware of news about threats to their privacy from their service providers or government agencies. This news may be disturbing to people unaccustomed to thinking of law enforcement or internet services as threatening. It might also be unpleasant for any frequent internet user to contemplate the various threats to her privacy. People may simply not process such troubling news if it is only heard once or quickly skimmed in the morning paper.

3. Rational Ignorance.—Remaining uninformed about basic aspects of politics, science, technology, and other aspects of life is rational behavior for many people. For example, it is economically rational for the average citizen to remain ignorant about politics and government policy, because the odds that she could affect the course of public policy via voting or other means of political participation are extremely small.[179] This phenomenon of *rational ignorance* extends to other areas of life.[180] Consumers rarely collect information about every aspect of their purchase decisions. Instead they learn a little bit about the food they eat, the cars they drive, and the politicians they support, and assume or ignore the rest.[181]

Consistent with rational ignorance, large portions of the public do not actually know many "well-known" facts. Only 36% of Americans can name all three branches of the United States government, while 35% cannot name a single branch.[182] Only 27% of Americans know that it takes

---

[176] *Id.*

[177] *Id.*

[178] C.H. SANDAGE ET AL., ADVERTISING THEORY AND PRACTICE 116–17, 187–88 (12th ed. 1989).

[179] *E.g.*, GUIDO PINCIONE & FERNANDO R. TESÓN, RATIONAL CHOICE AND DEMOCRATIC DELIBERATION: A THEORY OF DISCOURSE FAILURE 14 (2006).

[180] *See* HOLLEY H. ULBRICH, PUBLIC FINANCE IN THEORY AND PRACTICE 55 (2d ed. 2011).

[181] *Id.*

[182] ANNENBERG PUB. POL'Y CTR., *Americans Know Surprisingly Little About Their Government, Survey Finds* (Sept. 17, 2014), http://www.annenbergpublicpolicycenter.org/americans-know-surprisingly-little-about-their-government-survey-finds [https://perma.cc/J62H-3WC9].

a two-thirds vote of the House and Senate to override a presidential veto.[183] In 2014, only 38% of Americans knew which party controlled the Senate.[184] Americans likewise struggle with basic facts about science. Less than half know that electrons are smaller than atoms, according to a poll that asked a simple true/false question.[185] Only 20% know which gas makes up most of the Earth's atmosphere.[186] These are fundamental and widely publicized facts, and most people are, quite rationally, ignorant of them.

It can also be rational to ignore information about police practices or surveillance, because consumers are unlikely to have much use for such information. Information about surveillance of internet or cell phone activity is unlikely to cause consumers to stop using the internet or cell phones, because both have become integral parts of most people's daily routine.[187] Nor are consumers likely to have the opportunity to partially protect their internet or cell phone privacy at a reasonable cost in time or effort. Many scholars have noted that "privacy markets" where consumers can choose among products based on how well they protect privacy have largely failed to function.[188] Reasons for this failure include the prohibitively high costs of monitoring technology companies for privacy infractions and the related lack of a critical mass of privacy-savvy consumers.[189] As a result, consumers may be unable to use most

---

[183] *Id.*

[184] *Id.* (at the time of the survey, it was the Democratic Party).

[185] PEW RESEARCH CTR., PUBLIC'S KNOWLEDGE OF SCIENCE AND TECHNOLOGY (Apr. 22, 2013), http://www.people-press.org/2013/04/22/publics-knowledge-of-science-and-technology [https://perma.cc/MES5-ZFS7].

[186] *Id.* The answer is nitrogen.

[187] People use the internet for an incredible variety of important activities, which they are unlikely to forego even if faced with serious threats of surveillance. *See* Tokson, *supra* note 37, at 588–89 (consumers use the internet for many important purposes, including dating, entertainment, news gathering, political discourse, health, sex, and voting, among others). The internet is used by roughly 84% of all Americans, including nearly all Americans under thirty (96%) and nearly all Americans with a college degree (95%). PEW RESEARCH CTR., AMERICANS' INTERNET ACCESS: 2000–2015 (Jun. 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015 [https://perma.cc/X4G7-J9JH]. Similarly, approximately 91% of Americans own a cell phone, and cell phone use is so popular that users are worried about overusing them. Rainie, *supra* note 1; AARON SMITH, PEW RESEARCH CTR., THE BEST (AND WORST) OF MOBILE CONNECTIVITY (Nov. 30, 2012), http://www.pewinternet.org/2012/11/30/the-best-and-worst-of-mobile-connectivity/ [https://perma.cc/6BPZ-QALL]. For many households (roughly 36% as of 2012), the cell phone is the only phone—and as the Supreme Court noted long ago, phones play a "vital role . . . in private communication." Katz v. United States, 389 U.S. 347, 352 (1967); SMITH, *supra*.

[188] *E.g.*, Julie E. Cohen, *Irrational Privacy?*, 10 J. TELECOMM. & HIGH TECH. L. 241, 242 (2012). Note that salient privacy protections can, in some cases, differentiate products and lead to market success—perhaps the primary selling point of Snapchat is its (imperfect) privacy-protective features.

[189] *See, e.g.*, Paul M. Schwartz, *Privacy, Property, and Personal Data*, 117 HARV. L. REV. 2055, 2078–79 (2004). Moreover, the steps that consumers can currently take to differentiate among products based on privacy protection, like comparing privacy policies, are likely to be prohibitively costly. Scholars have estimated that reading privacy policies would result in a time cost to consumers of over

information about privacy to their advantage. As with knowledge about science or politics, public knowledge about surveillance and privacy threats is likely to be counterintuitively low.

4. The Uneven Distribution of Knowledge.—Knowledge tends to disseminate unevenly across a population, as certain groups of individuals gain knowledge more quickly than others. This uneven distribution of knowledge may raise questions of fundamental fairness in the Fourth Amendment context, where courts often attribute the knowledge of the average person to a particular criminal suspect.[190]

Research on how knowledge spreads has shown that knowledge about a new innovation, technology, or service tends to reach people with higher levels of education more quickly than those less educated.[191] The same is true of people of higher social status, income, and wealth.[192] This is exacerbated by the tendency of innovators, marketers, and scholars to ignore persons at the lower strata of education and wealth and focus on easier-to-reach elites.[193] Demographic gaps in knowledge about science and technology may be especially large.[194]

Judges, especially federal judges, are well above the median in terms of education and wealth.[195] They are likely better informed than the average person about things like the structure of government and basic political

---

$700 billion (roughly $3534 per internet user) per year for internet-based policies alone. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 564–65 (2008). Consumers may also have little incentive to protect against private sector surveillance, as opposed to police or government agency surveillance. Private entities that process personal information tend to store the information in anonymized form. *See, e.g.*, Tokson, *supra* note 37, at 607. Although anonymity is increasingly vulnerable to de-anonymization in the era of Big Data, it is likely that consumers will continue to perceive the capture of anonymous data as substantially less worrisome than that of easily traceable personal information. *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 tbl. (2008) (poll respondents rated anonymous record gathering less intrusive than nonanonymous record gathering). In addition, consumers may have little incentive to worry about private sector access to their personal information because private sector access tends to be fully automated. Tokson, *supra* note 37, at 602–09. Although consumers generally perceive human observation of their data to be invasive, they are far less concerned about automated scanning or the mere storage of their data on third-party servers. *Id.* at 619–29.

[190] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

[191] ROGERS, *supra* note 164, at 174.

[192] *Id.* at 174, 288, 464–65, 467.

[193] *Id.* at 456–57.

[194] *See* PEW RESEARCH CTR., PUBLIC'S KNOWLEDGE OF SCIENCE AND TECHNOLOGY, *supra* note 185 (describing survey results that demonstrate a strong correlation between education level—college attendance in particular—and knowledge about science and technology).

[195] *See, e.g.*, Andrew B. Coan, *Is There a Constitutional Right to Select the Genes of One's Offspring?*, 63 HASTINGS L.J. 233, 243 (2011) (noting that judges are substantially wealthier and better educated than the general population).

facts.[196] They are far more likely to read or be told about government surveillance programs and technologies. And they know exponentially more than the average person about criminal procedure law and policy.

Judges are accordingly not well positioned to intuit what most people know about their privacy. As discussed above, the level of public knowledge about many basic facts is counterintuitively low.[197] Judges, who rank high in education, wealth, and status, are likely to learn new information well before the average person.[198] As such, they are especially likely to err when using their intuition or experiences to determine what people know about new technologies and concepts. Facts that are already common knowledge among judges may not yet have reached people of average socioeconomic status, and indeed may never reach them.[199]

Criminal activity is correlated with lower income, education, and social status.[200] Moreover, law enforcement investigations often disproportionately target low-socioeconomic-status neighborhoods and areas.[201] If persons targeted by police investigations know less about new technologies or surveillance practices than the average American, then courts may be systematically overestimating the knowledge of the suspects who assert Fourth Amendment protection in criminal cases. For instance, a suspect from the lowest quintiles of income, education, and social class may lose her case because the judge inaccurately concludes that she possessed "common" knowledge about CSLI or email technology. These systematically inaccurate attributions of knowledge may, in turn, further diminish the perceived legitimacy of the criminal justice system among low-socioeconomic-status groups.[202]

Individuals from low-income, education, or social status groups may thus be doubly harmed in the law enforcement process. Not only are they more likely to be targeted by law enforcement, they are also more likely to

---

[196] *See* PEW RESEARCH CTR., WHAT THE PUBLIC KNOWS—IN PICTURES, WORDS, MAPS AND GRAPHS (Apr. 28, 2015), http://www.people-press.org/2015/04/28/what-the-public-knows-in-pictures-words-maps-and-graphs [https://perma.cc/86ZY-4B74] (showing that knowledge of basic facts about politics and the world is correlated with educational attainment).

[197] *See supra* Section III.A.3.

[198] *See supra* notes 195–97 and accompanying text.

[199] *See* ROGERS, *supra* note 164, at 174, 288, 456, 464–65, 467.

[200] *See, e.g.*, LEE ELLIS ET AL., HANDBOOK OF CRIME CORRELATES 32–42, 60–65 (2009).

[201] *See, e.g.*, Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809, 871–72 & n.232 (2011).

[202] For a discussion of the problems caused by the perceived illegitimacy of the criminal justice system, for example, Tracey L. Meares, *Norms, Legitimacy and Law Enforcement*, 79 OR. L. REV. 391 (2000).

lose Fourth Amendment protection on the basis of imputed knowledge that they do not possess.

B. Practical and Formal Problems

The conceptual difficulties inherent in the assessment of societal knowledge are not just a problem in the abstract. They frequently result in questionable or even provably wrong conclusions about knowledge in Fourth Amendment cases. This Section discusses these practical problems, the biases that are likely to affect judicial determinations of knowledge, and several examples of empirically incorrect conclusions about societal knowledge.

1. Waiver and the Phases of Knowledge.—Courts' failure to recognize the complex, multilevel nature of knowledge often leads them to find that people have knowingly waived their Fourth Amendment rights on very thin evidence. In many cases, a vague or general awareness of the possibility of personal data collection is sufficient to vitiate Fourth Amendment rights. For example, the Supreme Court held that dialed telephone numbers were not private in part because customers have "some awareness" that telephone companies can record their numbers, and because many phone books contain a page with text implying that companies can track harassing calls.[203]

Furthermore, some courts do not require direct evidence of actual societal awareness, only the potential for awareness evinced by available articles or blog posts.[204] The Eleventh Circuit, for instance, ruled that CSLI was unprotected by the Fourth Amendment on the basis that there were "publicly available facts" about cell towers and cell companies recording cell tower usage.[205] District courts have reached the same conclusion by citing the availability of news articles discussing cell phone tracking.[206] These news sources may not be prominent or widely read, and public exposure to the relevant information is likely quite limited.[207] Further, many people exposed to these news stories may not actually become aware of them, let alone understand their content.[208] At most, these courts have identified a possibility that some people might be aware of certain

---

[203] Smith v. Maryland, 442 U.S. 735, 742–43 (1979).

[204] *See In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 140 & n.19, 146 (E.D.N.Y. 2013) (finding public knowledge of CSLI based in part on a blog post discussing how the author tracked down his lost iPhone).

[205] *Davis II*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc).

[206] *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d at 140–41.

[207] *See id.*

[208] *See supra* Sections III.A–III.B.

information—but the mere potential for awareness is typically not sufficient grounds for the waiver of a constitutional right.[209]

2. Judicial Intuition and Biases.—Assertions that something is "common knowledge"[210] or that "[a]ny person . . . knows"[211] something are essentially empirical claims. Yet courts rarely support such claims with evidence and very rarely rely on empirical or poll data on public knowledge. Judges' usual approach is simply to make an intuitive judgment about collective knowledge, perhaps based on their knowledge or beliefs at the time of decision.[212]

This is problematic for several reasons. As discussed above, judges are well-informed socioeconomic elites who are likely to systematically overestimate societal knowledge.[213] Societal knowledge tends to be counterintuitively low, and tends to spread more quickly to elites than to the average citizen.[214]

Moreover, by the time they decide a case, judges will almost certainly know about the surveillance technology or practice in question no matter how obscure it is—because the parties will have informed them about it in detail in pleadings or briefs long before a decision is issued. This acquired knowledge is likely to bias judges' intuitive judgments about societal knowledge. Individuals tend to automatically impute their own knowledge to other people.[215] This is true even when the knowledge is confidential and others are extremely unlikely to know it.[216] The result is that knowledgeable

---

[209] *See* Miranda v. Arizona, 384 U.S. 436, 492 (1966) (reasoning that signing "a statement which contained a typed-in clause stating that [Miranda] had 'full knowledge' of his 'legal rights'" and understood that statements he made could be used against him did "not approach the knowing and intelligent waiver required to relinquish constitutional rights"). A person may affirmatively consent to a search in the absence of knowing and intelligent waiver, *Schneckloth v. Bustamonte*, 412 U.S. 218, 242–43 & n.31 (1973), but there was no consent given in the cases addressed here. It is possible that courts could infer consent based on the knowing disclosure of information to third parties, but that would require a knowing disclosure, not the mere theoretical possibility of knowledge.

[210] *E.g.*, California v. Greenwood, 486 U.S. 35, 40 (1988); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(c)–(d), 42 F. Supp. 3d 511, 517 (S.D.N.Y. 2014).

[211] United States v. McDonald, 100 F.3d 1320, 1327 (7th Cir. 1996) (alteration in original), *abrogated by* Bond v. United States, 529 U.S. 334 (2000).

[212] *See, e.g.*, *Greenwood*, 486 U.S. at 40; California v. Carney, 471 U.S. 386, 392 (1985); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

[213] *See supra* notes 195–96 and accompanying text.

[214] *See supra* Sections III.A.3–III.A.4.

[215] *See* Raymond S. Nickerson, *How We Know—and Sometimes Misjudge—What Others Know: Imputing One's Own Knowledge to Others*, 125 PSYCH. BULL. 737, 745–49 (1999) (gathering various studies indicating that people's estimates of what others know are systematically biased by what the estimators themselves know).

[216] *See* Boaz Keysar et al., *States of Affairs and States of Mind: The Effect of Knowledge of Beliefs*, 64 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 283, 284 (1995) ("[P]eople's tendency to

people overestimate, often severely, what others know.[217] Judges deciding Fourth Amendment cases based on their intuitions about knowledge are likely susceptible to the same biases.[218]

More generally, decisions based on empirical data are likely to be sounder and more accurate than decisions based on guesses about an empirical matter. Other scholars have criticized the Supreme Court for failing to seek out empirical data on citizens' future expectations of privacy, so I will not dwell on this point.[219] It is worth noting, however, how much more force this critique has in the context of an inquiry into knowledge. The reasonable expectation of privacy inquiry arguably contains a normative as well as an empirical element. It can be construed to ask not only what people do expect in the future but what they have a right to expect.[220] But courts assessing collective knowledge are making a more straightforward empirical determination: what people know in the present day. Courts drawing empirical conclusions about societal knowledge without any empirical evidence is thus especially troubling. It is also particularly dangerous, because courts' empirical assertions may be proven wrong by new evidence. If the empirical conclusions about collective knowledge that form the basis for many Fourth Amendment decisions turn out to be incorrect, the result may be instability and unpredictability in Fourth Amendment law and further harm to the legitimacy of the justice system.

3. Empirical Data on Societal Knowledge.—There is a dearth of empirical information on the extent of societal knowledge about surveillance practices or new technologies. However, the studies that do exist indicate that courts have decided several important Fourth

behave as if others have access to their own privileged information—even when they are fully aware they do not").

[217] *Id.* at 283–84; Nickerson, *supra* note 215, at 745–49.

[218] *See generally* Chris Guthrie, Jeffrey J. Rachlinski & Andrew J. Wistrich, *Inside the Judicial Mind*, 86 CORNELL L. REV. 777, 784, 829 (2001) (describing the results of a study indicating that judges are likely to exhibit the same biases as non-judges). Further, societal knowledge may itself change over the several years that it may take for a case to be resolved, especially if the case goes through one or more rounds of appeals. A new technology that was largely unknown at the time of the initial police search might be well known by the time an appeals court rules on the constitutionality of the search.

[219] *See, e.g.*, Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*," 42 DUKE L.J. 727, 757–58 (1993).

[220] *See* LEE, *supra* note 73, at 238–42; Kerr, *supra* note 19, at 507–22. Nonetheless, the most common application of the *Katz* test is simply to inquire about society's actual expectations of privacy. *See* Simmons, *supra* note 125, at 586 n.108.

Amendment cases on the basis of demonstrably erroneous conclusions about societal knowledge.

a. User knowledge and the internet.—Courts have held that internet users have relatively detailed knowledge about how the internet works, how emails are processed and monitored, and how ISPs collect and store personal information.[221] Studies examining people's actual knowledge of internet data privacy suggest that courts are substantially overestimating such knowledge.[222] For example, a recent Consumer Reports poll found that 61% of internet users incorrectly think that what they do online is never shared without their permission, while 57% erroneously think that companies gathering internet data must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations.[223] Courts should be cautious in assuming that internet users understand that ISPs may collect their personal or web surfing information.

Many courts rely on consumers' supposed knowledge of ISP privacy policies addressing the collection or sharing of personal data. They conclude that knowledge of policies that permit data gathering "may well extinguish [a user's] reasonable expectation of privacy."[224] Courts have relied on privacy policies to determine the extent of user knowledge in cases involving email content,[225] web surfing activity,[226] subscriber information,[227] and cell phone location data.[228] But courts' assumption that users are at least generally aware of the contents of their privacy polices is empirically incorrect. In fact, users are very unlikely to read their privacy policies, and most users do not understand what a "privacy policy" is.[229]

---

[221] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (concluding that internet users know that their email and IP addresses are used by third parties to route internet information); United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *3 (4th Cir. Aug. 3, 2000) (per curiam) (stating that an internet user knowingly revealed his subscriber information to his ISP and its employees).

[222] *See infra* notes 223–35 and accompanying text.

[223] *Poll: Consumers Concerned About Internet Privacy*, CONSUMERSUNION.ORG (Sept. 25, 2008), https://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy [https://perma.cc/MHJ2-5UKW].

[224] *Warshak I*, 490 F.3d 455, 473 (6th Cir. 2007), *vacated en banc on ripeness grounds*, *Warshak II*, 532 F.3d 521 (6th Cir. 2008). This assumption about user knowledge dates back to *Smith v. Maryland*, where the Supreme Court assumed that telephone users were aware of the contents of a "Consumer Information" page in most telephone books. 442 U.S. 735, 742–43 (1979).

[225] *E.g.*, *Warshak III*, 631 F.3d 266, 287 (6th Cir. 2010).

[226] *E.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007).

[227] United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005).

[228] *E.g.*, *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013).

[229] *See infra* notes 230–35 and accompanying text.

A privacy policy is a statement that discloses a company's policy on collecting and using personal information.[230] Yet the majority of internet users (55–59%) erroneously believe that the existence of any "privacy policy" means that their information will be kept private.[231] These users likely feel that they have no reason to read the contents of privacy policies.[232] Furthermore, even sophisticated users are unlikely to read privacy policies because reading privacy policies would be prohibitively laborious. Scholars have estimated that reading internet-based privacy policies alone would take roughly 244 hours annually for each internet user.[233] Very few internet users—about 3% in one survey and 1.4% in another—report reading most privacy policies or user agreements (which often contain privacy policies).[234] A study of visitors to certain software retail websites revealed that only 0.14% of those who purchased software read or skimmed the applicable user agreement.[235]

In short, there is no empirical evidence that people are aware of the contents of their privacy policies, and substantial evidence to the contrary. The numerous, often important court cases that rely on privacy policies as a barometer of consumer knowledge are premised on a highly questionable assumption.[236]

b. User knowledge and location surveillance.—Numerous courts have decided cell phone location tracking cases based on assessments of societal knowledge. A majority of federal courts have concluded that most people know that cell phone companies regularly record information about

---

[230] Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 723, 731 (2007–2008) (explaining what privacy policies disclose).

[231] *Id.* at 735.

[232] *Id.* at 747.

[233] McDonald & Cranor, *supra* note 189, at 563.

[234] Turow et al., *supra* note 230, at 740; Brief for Kelly Caine et al. as Amici Curiae in Support of Petitioners' Motion of Objection to March 11, 2011 Order Denying Motion to Vacate and Denying in Part Motion to Unseal at 4, *In re* Application of U.S. for Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114 (E.D. Va. 2011) (Misc. Nos. 11-DM-00003 & 10GJ3793).

[235] Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 20 (2014) (finding that 7 out of 4866 purchasers read or skimmed the applicable user agreement). Further, for those who accessed the agreements, the median viewing time was only sixty seconds. *Id.*

[236] *See, e.g.*, *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (finding that users know that cell phone companies gather and store data about their location based on privacy policies); *Warshak III*, 631 F.3d 266, 287 (6th Cir. 2010) (holding that a user's expectation of privacy in her email content turned on the applicable privacy policy); *see also* Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (finding that telephone users know the contents of the informational material in telephone books).

users' locations.[237] Accordingly, these courts hold that cell phone users have knowingly exposed their location data and therefore forfeited any Fourth Amendment protection.[238] But courts' assertions about societal knowledge are not based on empirical data—indeed little direct empirical data exists about people's knowledge of cell phone technology and surveillance. To fill this gap and assess the accuracy of courts' assertions about collective knowledge of cell phone technology, I conducted a survey of 810 cell phone users. The survey's findings cast doubt on the validity of the majority of cell phone location tracking cases.

A sample of 810 adult cell phone users living in the United States was recruited using Amazon's Mechanical Turk service.[239] Four respondents were excluded for failure to plausibly answer a screening question.[240] This sample was not census-weighted, and was younger, more male, and had slightly higher levels of educational attainment than the general U.S. population.[241] The gender of 46.5% of respondents was female. The age of

---

[237] *See, e.g.*, *Davis II*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) ("[C]ell users know . . . that users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower's range, and that cell phone companies make records of cell-tower usage."); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(c)–(d), 42 F. Supp. 3d 511, 518 (S.D.N.Y. 2014) ("[S]ubscribers are aware that use of their cell phones necessitates disclosure of the information sought."); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y. 2013) (citing *In re* Application of U.S. for Order Authorizing Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011)) ("[I]t is clearly within the knowledge of cell phone users that their telecommunication carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time."); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012) (It is "common knowledge that communications companies regularly collect and maintain all types of non-content information regarding cell-phone communications, including cell-site tower data, for cell phones for which they provide service.").

[238] *See, e.g.*, *Davis II*, 785 F.3d at 511 (determining that cell phone users' knowledge of how cell phones work means that they lack a reasonable expectation of privacy in their location information); *In re Application of U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(c)–(d)*, 42 F. Supp. 3d at 517–18 (holding that cell phone users' awareness of the disclosure of their cell phone information undermines any Fourth Amendment protection for such information).

[239] For more details on Mechanical Turk's survey recruiting service, see generally Michael Buhrmester, Tracy Kwang & Samuel D. Gosling, *Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?*, 6 PERSPS. ON PSYCHOL. SCI. 3 (2011). The website is frequently used to conduct surveys by legal scholars and social scientists. *See, e.g.*, David A. Hoffman & Tess Wilkinson-Ryan, *The Psychology of Contract Precautions*, 80 U. CHI. L. REV. 395, 409–10 (2013) (reporting a survey on preferences for warranties and liquidated damages clauses in contracts); Stuart P. Green & Matthew B. Kugler, *Public Perceptions of White Collar Crime Culpability: Bribery, Perjury, and Fraud*, 75 LAW & CONTEMP. PROBS. 33, 41–42 (2012) (reporting a survey on the perceived blameworthiness and preferred punishments for different bribery scenarios).

[240] The question asked the name of their current cell phone service provider.

[241] In a recent study using Mechanical Turk, survey respondents were younger, more male, and had higher preferences for privacy than the general population. Matthew B. Kugler & Lior Strahilevitz, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory* 47 (Coase-Sandor Working Paper Series in Law & Economics No. 727, 2015), http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2419&context=law_and_economics

43.8% of respondents was thirty-five or older.[242] The highest level of education for 9.6% of respondents was a graduate degree, 37.1% a bachelor's degree, 15.8% an associate's degree, and 37.1% a high school degree. The household income of 58.4% of respondents was below $50,000.[243]

Contrary to courts' conclusions about collective knowledge of cell phone tracking, this survey indicates that the majority of cell phone users do not know that their cell phone provider collects their location data, and roughly 15% of users affirmatively believe that their data is not collected. Participants were asked whether their cell phone service provider regularly collects information on their physical location using their cell phone.[244] Nearly three-quarters of participants (73.5%) answered either "No" (15.0%) or "I Don't Know" (58.5%) to this question, compared to 26.5% who answered "Yes." Moreover, most of the 213 respondents who answered "Yes" referred to GPS or Google Maps in a follow-up explanation, while only 27 respondents referenced anything that could be construed as involving cell site location tracking.[245] This suggests that very few users (only 3.3% of all respondents) are aware of the cell site location information at issue in most cell phone surveillance cases.

[https://perma.cc/JE8E-CDMU]. Assuming that this Article's sample has similarly high privacy preferences, the overall sample may have sought more information about potential threats to privacy than the general population. However, the survey respondents here were generally not knowledgeable about CSLI and did not read their privacy policies. The general population may be even less informed.

[242] In total, 56.2% of respondents were between ages 18–34, 36.2% were between ages 35–54, and 7.6% were over age 55. In the general U.S. population as of 2010, 50.8% of people were female, and the median age was 37.2. LINDSAY M. HOWDEN & JULIE A. MEYER, U.S. CENSUS BUREAU, AGE AND SEX COMPOSITION: 2010, at 2 & tbls.1 & 2 (May 2011), http://www.census.gov/prod/cen2010/briefs/c2010br-03.pdf [https://perma.cc/ZC4G-MVT2].

[243] In the general U.S. population age 25 or older, the highest level of educational attainment for 12.0% of people was an advanced degree, 20.5% a bachelor's degree, 9.8% an associate's degree, and 46.1% a high school degree. *See* CAMILLE L. RYAN & KURT BAUMAN, U.S. CENSUS BUREAU, EDUCATIONAL ATTAINMENT IN THE UNITED STATES: 2015, at 2 tbl.1, (Mar. 2016), https://www.census.gov/content/dam/Census/library/publications/2016/demo/p20-578.pdf [https://perma.cc/MGE3-GCVN]. In the U.S., 46.8% of households had an income below $50,000 in 2014. U.S. CENSUS BUREAU, CURRENT POPULATION SURVEY, ANNUAL SOCIAL AND ECONOMIC SUPPLEMENT, at tbl. HINC-06 (2015), https://www.census.gov/data/tables/time-series/demo/income-poverty/cps-hinc/hinc-06.html [https://perma.cc/3Y6V-P5BX].

[244] The exact phrasing was "Does your cell phone service provider regularly collect information on your physical location using your cell phone?" This question was phrased broadly enough to encompass GPS tracking as well as cell site location recording, and thus responses may overestimate societal knowledge about cell site location tracking.

[245] Participants who responded "Yes" when asked about location tracking were given an open-ended prompt that asked, "Please describe how your cell phone service collects information on your physical location." Any response that could reasonably be interpreted as referring to CSLI was coded as doing so. Such responses varied widely in terms of detail, from "collects via making call" to "It can approximate my location by determining which cell tower is being used, which would be the cell tower closest to me."

TABLE 1: SURVEY RESPONSES, CELL PHONE LOCATION TRACKING

Does your cell phone provider regularly collect information on your physical location using your cell phone?		
Yes	**No**	**I Don't Know**
26.5%	15.0%	58.5%

TABLE 2: FOLLOW-UP QUESTION FOR RESPONDENTS ANSWERING YES

Please describe how your cell phone service collects information on your physical location.	
Answer could be construed as referring to CSLI	**Answer could not be construed as referring to CSLI**
12.7%	87.3%

Further, and contrary to the assumptions of several courts in location tracking cases,[246] the vast majority (89.8%) of respondents reported that they have not read or skimmed in detail their cell phone service's privacy policy. By contrast, 7.3% report that they have skimmed the policy in detail, and 2.9% say they have read all or most of it.[247]

[246] *See, e.g.*, *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (footnote omitted) (noting that privacy policies "inform subscribers" that providers use "a subscriber's location information to route his cell phone calls [and] collect it"); United States v. Graham, 846 F. Supp. 2d 384, 401 (D. Md. 2012) ("[A]ny assumption of ignorance is belied by Sprint/Nextel, Inc.'s privacy policy, which informs its customers that it collects location data.").

[247] Nearly half of respondents (46.7%) reported skimming their privacy policy briefly, and 43.1% reported that they were unaware of it, did not want to read it, or were unable to access it. Participants were initially asked "Have you read your cell phone service provider's official privacy policy?"

Note that privacy policies are generally written in dense, legalistic language unlikely to be understood even by internet users who skim policies in depth. *See* Carlos Jensen & Colin Potts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, *in* 6 PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 471, 475 (2004).

TABLE 3: SURVEY RESPONSES, PRIVACY POLICIES

Have you read your cell phone service provider's official privacy policy?			
I have read all or most of it	**I have skimmed it in a detailed manner**	**I have skimmed it briefly**	**I was unaware of it, did not want to read it, or was unable to access it**
2.9%	7.3%	46.7%	43.1%

This is this first study to directly measure cell phone users' knowledge of location tracking, and there remains a need for additional surveys to confirm its results. But the results of the study suggest that many courts have imputed knowledge about cell phone technology and surveillance practices that users do not possess. This is not the result of any doctrinal error—these courts are amply supported by precedent when they look to collective knowledge to determine the Fourth Amendment's scope.[248] Rather, the problems inherent in the search for societal knowledge and the practical difficulties of assessing it have combined to lead judges astray in the majority of federal cell phone tracking cases. If this trend continues, the Fourth Amendment's boundaries will be drawn based on empirical conclusions that are deeply flawed.

C. Improving the Assessment of Societal Knowledge

Courts could, in theory, take a far more empirical approach to determining societal knowledge in Fourth Amendment cases. They could rely on surveys that measure people's knowledge of relevant technologies or surveillance techniques rather than relying on intuition or the contents of privacy policies. This would likely produce more accurate conclusions about societal knowledge than courts' current approaches.

In addition, surveys designed primarily to test knowledge rather than evaluate opinions would likely avoid many of the drawbacks of standard opinion polls. Surveys often ask people for positions on issues that they

[248] *See, e.g.*, *Davis II*, 785 F.3d 498, 511–12 (11th Cir. 2015) (en banc) (drawing a direct parallel to Smith v. Maryland, 442 U.S. 735 (1979)).

have never considered in any depth.[249] People will do their best to give an answer, but their answer may not reflect a meaningful opinion on the issue. Accordingly, public poll responses often do not match people's behavior.[250] Relatedly, when people do not have firm opinions on an issue, their responses may vary substantially based on the perspective of the question asked.[251] This can result in opinion polls on the same issue producing contradictory results.[252] Thus public ignorance or ambivalence can undermine opinion polls, especially those addressing complex or subtle issues.[253] By contrast, surveys that quiz people to determine whether they know something are less vulnerable to these framing effects. Further, public ignorance about a topic cannot undermine knowledge-focused surveys—public ignorance is exactly what these surveys seek to measure.

In practice, courts deciding novel Fourth Amendment cases are often unable to rely on survey data because scholars or pollsters rarely collect such data until after several courts, and often the Supreme Court, have already weighed in on the issue. This might be mitigated through unconventional measures like providing federal courts with a budget to conduct surveys of public knowledge through polling services like Amazon Mechanical Turk, Toluna, or Qualtrics. The decreasing cost of obtaining survey data may also encourage scholars to regularly collect and publish data on public knowledge of privacy-relevant technologies and issues.[254]

To whatever extent they are available, the increased use of empirical studies of public knowledge would likely improve the quality and validity of courts' Fourth Amendment decisions. But even if courts could improve their assessments of knowledge, there are potentially serious flaws inherent in a knowledge-based Fourth Amendment regime. The next Part examines whether, even if courts could better assess societal knowledge, they should nonetheless abandon the use of societal knowledge as a determinant of the Fourth Amendment's scope.

---

[249] *See, e.g.*, John Zaller & Stanley Feldman, *A Simple Theory of the Survey Response: Answering Questions Versus Revealing Preferences*, 36 AM. J. POL. SCI. 579, 579–80 (1992).

[250] *See* Solove, *supra* note 25, at 1522–23.

[251] *See* Zaller & Feldman, *supra* note 249, at 582–83, 585.

[252] *See, e.g.*, *id.* at 581–83 (describing studies where different orderings of the same questions produced substantially different results and where the same respondents gave different answers in surveys given only months apart).

[253] *Id.* at 582–84.

[254] *Cf.* Kugler & Strahilevitz, *supra* note 241 (reporting results of surveys asking respondents about their expectations of privacy in certain situations). As part of their project, Kugler and Strahilevitz hope to collect and publish additional relevant data annually. *Id.* at 27 n.136.

IV. KNOWLEDGE AND THE EROSION OF THE FOURTH AMENDMENT

Assessing societal knowledge in the Fourth Amendment context is fraught with difficulty. Empirical evidence indicates that courts have badly overestimated societal knowledge in a variety of areas.[255] But such failure is not inevitable, at least in theory.[256] This Part considers whether even accurate assessments of societal knowledge should play a role in setting the boundaries of the Fourth Amendment.

A. The Importance of Knowledge Gaps Under Current Law

Knowledge of a new concept or fact often spreads slowly, passing from person to person through social networks and political hierarchies.[257] It may take years for most people to learn about new information, and many ideas will never reach a majority of the population.[258]

As threats to privacy continue to proliferate, these gaps in collective knowledge offer a zone of privacy protection under the knowledge-based *Katz* inquiry. If anything, knowledge's role in Fourth Amendment law is likely to grow as surveillance technologies advance and private entities are able to collect, process, and store new types of personal information.[259] In a world where private entities can access emails, web surfing data, files in cloud storage, detailed location information, and video feeds from millions of sources, users' lack of detailed knowledge about threats to their privacy may be the primary remaining source of reasonable privacy expectations.

As discussed above, public knowledge is often remarkably low, and the average person may rationally fail to become aware of publicly available and potentially useful information.[260] A Fourth Amendment based on citizens' lack of knowledge is not inherently unworkable. People will remain ignorant about the collection of their personal information and other threats to their privacy, even when such information is known to privacy experts or informed elites. But such a regime—which Fourth Amendment law is increasingly coming to resemble—is inherently unstable. Not only does it risk inconsistent and unfair results, but its protections are also likely to shrink over time as people become more knowledgeable about technology and surveillance.

---

[255] *See supra* Section III.B.2.

[256] *See supra* Section III.C.

[257] *See* BEAL & BOHLEN, *supra* note 165, at 3–4.

[258] *See, e.g.*, ROGERS, *supra* note 164, at 1–5, 171–72, 227–28.

[259] For a discussion of the rapid advance of surveillance technology and private entities' extensive access to citizens' personal information, see Ohm, *supra* note 130, at 1310.

[260] *See supra* Section III.A.3.

B. Rapid Changes in Societal Knowledge

Public knowledge about a given threat to privacy can spike dramatically due to unpredictable events. High-salience news stories that involve new technologies or surveillance techniques may rapidly disseminate privacy-relevant information to the public.[261] For example, the O.J. Simpson case may have sharply increased public awareness of DNA blood testing techniques.[262] But the incidence and timing of national news stories that reveal privacy-relevant information can be very difficult to predict.

Likewise, public ignorance about threats to privacy can be undermined by leaks from government or private actors. An especially high-profile leak, like Edward Snowden's release of NSA documents detailing various mass surveillance programs, may sharply increase public awareness of privacy threats, potentially leading to changes in societal expectations of privacy.[263] Yet many revelations about privacy threats will fail to capture public attention. National newspapers reported on the existence of the NSA's massive telephone metadata collection program as early as 2006.[264] But the program did not garner widespread media attention

---

[261] *See* sources and discussion *infra* note 263.

[262] DNA blood testing played a major role in the O.J. Simpson trial, which was followed closely by large segments of the American public. *See, e.g.*, GALLUP–CNN/USA TODAY, *The O.J. Simpson Trial: Opinion Polls*, http://law2.umkc.edu/faculty/projects/ftrials/Simpson/polls.html [https://perma.cc/YR7U-D98J] (reporting that a 1995 Gallup poll found that 80% of Americans watched the Simpson trial verdict).

[263] A May 2014 poll found that 71% of Americans had seen, read, or heard news coverage about Edward Snowden, with 38% having seen a lot and 33% having seen just some. HART RESEARCH ASSOCIATES/PUBLIC OPINION STRATEGIES, NBC NEWS NATIONAL SURVEY (May 27–29, 2014), http://msnbcmedia.msn.com/i/MSNBC/Sections/A_Politics/14353%20May%20NBC%20News%20National%20Survey%20Interview%20Schedule.pdf [https://perma.cc/7UMA-UC54]. Familiarity with such programs remains high in 2015, with 87% of people reporting awareness of the government's telephone and internet surveillance programs, 31% having heard a lot about it, and 56% having heard at least a little. LEE RAINIE & MARY MADDEN, PEW RESEARCH CTR., AMERICANS' PRIVACY STRATEGIES POST-SNOWDEN (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden [https://perma.cc/S9LV-ZS49].

It remains unclear whether revelations about government surveillance programs, as opposed to private surveillance practices, can themselves erode people's reasonable expectations of privacy. The Supreme Court has said that the police cannot destroy expectations of privacy by simply announcing that they will henceforth conduct random searches of people's homes. Smith v. Maryland, 442 U.S. 735, 740–41 n.5 (1979). However, the Court has often found that noncriminal government surveillance practices can reduce people's reasonable expectations of privacy. *See, e.g.*, California v. Carney, 471 U.S. 386, 392 (1985) (finding that public expectations of privacy in cars are reduced because of public knowledge of the government's extensive regulation of cars). One possibility is that government surveillance programs that are deemed justifiable on national security grounds may be leveraged to reduce Fourth Amendment protections against domestic police surveillance.

[264] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006, 10:38 AM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm [https://perma.cc/Y9U9-9F3G].

until news of the program became associated with the dramatic details of Snowden's pilfering classified documents and fleeing the United States.[265] As with high-profile celebrity criminal cases, predicting when government or private actors will leak sensitive information or when such leaks will capture the media's attention would be virtually impossible.

Accordingly, the protections afforded by a knowledge-based Fourth Amendment regime are inherently unstable and the loss of Fourth Amendment protection unpredictable. The results produced by such a regime are also normatively unappealing. As discussed above, courts have relied heavily on assessments of knowledge in resolving the important question whether the Fourth Amendment protects people's cell site location information (CSLI).[266] Such information can reveal so much intimate information about a person's life at such low cost that it risks "alter[ing] the relationship between citizen and government in a way that is inimical to democratic society."[267] As the survey discussed in Section III.B.3 indicates, public knowledge of CSLI is currently very low, despite the profusion of federal and state criminal cases that involve cellular location tracking. Yet public knowledge could easily spike if CSLI evidence were a key part of the criminal case against a major celebrity or notorious criminal.[268] It is odd to say that the government should be able to warrantlessly track citizens' locations and obtain intimate details about their lives because a major news story happened to involve CSLI. This is reinforced by the fact that, even with increased awareness, consumers are unlikely to stop using their cell phones and may be unable to effectively prevent privacy invasions.[269] Such

---

[265] *See supra* note 263.

[266] *See supra* Section II.E.

[267] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S. Ct. 1534 (mem.) (2012)); *see also* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("[One] who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband . . . an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."); People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 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.").

[268] Public knowledge might also increase substantially if a previous crime case became the subject of a hit movie. This is not entirely hypothetical, as producers have explored making the popular podcast *Serial*, which discussed police use of cell phone location data, into a movie. *See* Joanna Robinson, *Hollywood Wants to Make a Movie Out of* Serial*. But Should They?*, VANITY FAIR (Nov. 20, 2014, 1:09 PM), http://www.vanityfair.com/hollywood/2014/11/serial-made-into-a-movie [https://perma.cc/KM7F-7T75].

[269] *See supra* notes 187–89 and accompanying text. In addition, the use of cell phone signals to locate cell phone users is a fundamental part of cellular phone systems. *See supra* Section II.E.1.

a major decision about the relationship between the government and its citizens should not turn on chance events.

C. The Expansion of Societal Knowledge

Societal knowledge is also a problematic basis for Fourth Amendment scope because knowledge about technology and surveillance practices is likely to increase over time. As people become better informed about threats to their privacy and the exposure of their information to others, their reasonable expectations of privacy will diminish.[270] This dynamic also makes it difficult to protect privacy through education or political action because, paradoxically, informing citizens about privacy threats can lead to reduced constitutional protection. Over time, a Fourth Amendment based on collective knowledge will shrink in scope, protecting ever fewer types of personal information and becoming increasingly irrelevant to the regulation of police behavior.

Available evidence suggests that technology knowledge is growing and will continue to grow as millennials and their successor generations replace older generations. Numerous studies report that younger people, especially the "digital natives" who have lived their entire lives in the internet age, know more about new technologies and computers than older people.[271] Young Americans are more likely to use the internet, to own smartphones, and to use smartphones for a wide variety of tasks like online banking, researching a health condition, and GPS navigation.[272] Younger demographic groups have also been shown to read technology news at higher rates than older groups.[273] Societal knowledge of technology will

---

[270] To be sure, many people will remain rationally ignorant about privacy threats and new technologies. But for the reasons set out in this Section, people are increasingly likely to acquire technology knowledge for nonprivacy purposes, and such knowledge may also inform them of privacy threats. Nor does rational ignorance entirely prevent citizens from acquiring information about their government or the world around them—many people just like to know, even if they are unlikely to profit from the knowledge.

[271] *See, e.g.*, PEW RESEARCH CTR., PUBLIC'S KNOWLEDGE OF SCIENCE AND TECHNOLOGY, *supra* note 185 (noting that younger Americans are more aware of nanotechnology and how lasers work than older Americans); PEW RESEARCH CTR., PUBLIC KNOWS BASIC FACTS ABOUT POLITICS, ECONOMICS, BUT STRUGGLES WITH SPECIFICS (Nov. 18, 2010), http://www.people-press.org/2010/11/18/public-knows-basic-facts-about-politics-economics-but-struggles-with-specifics [https://perma.cc/7KQ7-5GF5] (explaining poll finding that younger people are over three times as likely to identify Android as Google's smartphone operating system as older people).

[272] PEW RESEARCH CTR., INTERNET USER DEMOGRAPHICS (Jan. 2014), http://www.pewinternet.org/data-trend/internet-use/latest-stats [https://perma.cc/3ND3-EKC5]; Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ [https://perma.cc/ETR8-ZWJT].

[273] PEW RESEARCH CTR., 2008 PEW RESEARCH CENTER FOR THE PEOPLE AND THE PRESS NEWS CONSUMPTION AND BELIEVABILITY STUDY 49, http://www.people-press.org/files/legacy-pdf/444.pdf [https://perma.cc/M53J-J4AZ].

likely grow as these younger citizens replace the less tech-savvy baby boomers and as even more tech-literate generations are born.

More broadly, it is also likely that Americans' inherent capacity for knowledge will continue to increase over time. The citizens of advanced nations including the United States have experienced massive gains in IQ over the past century. From the early 1900s to the present day, Americans have gained roughly three to five IQ points per decade on standard tests.[274] Americans' educational attainment has also increased dramatically since the mid-twentieth century. In 1940, 75.9% of Americans over twenty-four had less than a high school education, 19.6% had completed high school or some college, and 4.6% had a bachelor's degree or higher. In 2015, only 11.7% of Americans over twenty-four had less than a high school degree, 56.4% had completed high school or some college, and 32.0% had a bachelor's degree or higher.[275] Studies have found that education is the strongest demographic predictor of knowledge about science and technology, with college-educated individuals substantially more knowledgeable than those with no college experience.[276]

In addition, the internet and other new communication technologies may lower the cost of acquiring information and increase the rate at which new information can disseminate throughout a population.[277] Not only can the internet facilitate mass communication, but it also decreases the costs of one-on-one communication and small-group communication over long distances.[278]

Awareness may also grow due to people's increasing interaction with information-collecting technologies. For instance, targeted emails, online

---

[274] James R. Flynn, *Are We Really Getting Smarter?*, WALL ST. J. (Sept. 21, 2012, 9:10 PM), http://www.wsj.com/articles/SB10000872396390444032404578006612858486012 [https://perma.cc/U6MT-BC9K].

[275] U.S. CENSUS BUREAU, PERCENT OF POPULATION AGE 25 AND OVER BY EDUCATIONAL ATTAINMENT: 1940–2015, at fig.2, http://www.census.gov/hhes/socdemo/education/data/cps/historical/fig2.jpg [https://perma.cc/3ULD-ECPA]. The rise in education levels has continued over the past decade. For instance, the number of men earning advanced degrees increased 27.1% from 2005 to 2015, and the number of women with advanced degrees rose 55.4%. U.S. CENSUS BUREAU, PERCENT CHANGE FROM 2005 TO 2015 IN THE NUMBER OF MEN AND WOMEN 25 AND OVER WHO HAVE COMPLETED SELECTED LEVELS OF EDUCATION, at fig.3, http://www.census.gov/hhes/socdemo/education/data/cps/historical/fig3.jpg [https://perma.cc/45DG-2WNM]. Note that some of this increase is the result of population growth, which was about 8.4% over the same time period. WORLD BANK, DATA: UNITED STATES, http://data.worldbank.org/country/united-states [https://perma.cc/4CNZ-H3CM].

[276] PEW RESEARCH CTR., PUBLIC'S KNOWLEDGE OF SCIENCE AND TECHNOLOGY, *supra* note 185.

[277] ROGERS, *supra* note 164, at 216.

[278] *Id.* Rates of internet use are high in America, at roughly 87.4%. WORLD BANK, INTERNET USERS (PER 100 PEOPLE), http://data.worldbank.org/indicator/IT.NET.USER.P2 [https://perma.cc/BSW6-XGLZ].

advertisements, and advertisements that reference internet users' prior purchases will raise awareness that online behavior is tracked and recorded.[279] To be sure, most people are unlikely to know the details of how their information is collected or tracked.[280] But even general knowledge has often been sufficient to eliminate Fourth Amendment protection.[281] Such general societal awareness about new technologies and surveillance techniques is likely to increase as information-collection practices proliferate.

To be sure, as new technologies and surveillance techniques are developed, new gaps in societal knowledge will arise that may provide the basis for Fourth Amendment protection under the current test.[282] But as people become more intelligent, better educated, better informed about science and technology, and have better access to new information, these gaps will close ever more rapidly.

A knowledge-based Fourth Amendment also makes it more difficult to protect privacy through political activism, because educating citizens about privacy threats may itself lead to diminished constitutional protection. This places privacy advocates in something of a double bind. Educating citizens about threats to their privacy may help them to take steps to protect their personal information from government surveillance. Likewise, raising awareness about surveillance is a crucial first step towards generating political momentum for legislative privacy protections.[283] But the more that citizens are informed of government

---

[279] Leary, *supra* note 5, at 367.

[280] *Id.*

[281] *See, e.g.*, *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 612–13 (5th Cir. 2013) (citing United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012)) (finding no Fourth Amendment protection for CSLI because "[a] cell service subscriber . . . understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call"); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (finding no Fourth Amendment protection for email or IP addresses because users should know that this information is used by their ISPs).

[282] *See supra* Section IV.A.

[283] There are currently several pro-privacy groups engaged in awareness raising and general advocacy efforts in support of proposed legislation. Yet these efforts may be counterproductive if they raise awareness of privacy threats but fail to result in effective legislative privacy protection.

The ACLU is currently leading an effort in sixteen states to pass legislation that protects internet privacy as part of its #TakeCTRL legislative program. Jose Pagliery, *ACLU Unveils Privacy Fight in 16 States*, CNN MONEY (Jan. 21, 2016, 11:53 AM), http://money.cnn.com/2016/01/20/technology/aclu-state-privacy-laws [https://perma.cc/S2UC-N9LY]. The Electronic Frontier Foundation promotes pro-privacy student activism and engages in several educational and awareness-raising efforts. *See About EFF*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about [https://perma.cc/32VP-2NN4]. The Electronic Privacy Information Center "educates the public and policymakers through the documents [obtained] through FOIA litigation." *EPIC Domestic Surveillance Project*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/surveillance [https://perma.cc/U2NB-E5GA].

surveillance programs and other threats to their privacy, the less likely they are to reasonably expect privacy in their personal information.[284] Grassroots efforts to support pro-privacy legislation are accordingly fraught with peril under the current legal regime. If they are unsuccessful, not only do they fail to enact new legislative privacy protections, but they may erode existing constitutional protections by increasing societal awareness of privacy threats.

Increases in knowledge about threats to privacy are especially problematic because of the low likelihood that such knowledge will motivate individuals to curtail their use of cell phones or the internet. As discussed above, these technologies have become integral parts of daily life.[285] Markets for privacy-protecting products have largely failed to develop, and consumers may have little incentive to seek out such products if their personal information is typically exposed only to automated systems.[286] Moreover, some privacy vulnerabilities are inherent in certain communications technologies.[287] It is hardly reasonable to force people to abandon important modes of communication or else forfeit their right to privacy—that is perhaps the central lesson of *Katz* itself.[288]

Even if judges administer it accurately, a knowledge-based Fourth Amendment is inherently unstable and prone to shrink over time as societal knowledge increases. It penalizes citizens for becoming informed about privacy threats and impedes political action to address such threats. The next Part explores some alternative approaches to Fourth Amendment scope.

V. A FOURTH AMENDMENT WITHOUT SOCIETAL KNOWLEDGE

This Part proposes that courts abandon the use of societal knowledge as a determinant of Fourth Amendment scope and explores some of the implications of doing so. Building on existing case law and scholarship,[289] it then offers two alternative models for drawing the boundaries of the Fourth Amendment. A comprehensive account of these models is beyond the scope of this Article, but this Part gives an overview of the models,

---

[284] *See* cases discussed *supra* Part II.

[285] *See supra* notes 187–89 and accompanying text.

[286] *See id.*

[287] For instance, any cell phone system will use towers situated at known locations, and the use of such towers creates the potential for government location tracking. *See supra* Section II.E.1.

[288] *See* Katz v. United States, 389 U.S. 347, 352 (1967) (stating that the telephone plays a "vital role . . . in private communication" and its users are entitled to privacy).

[289] *See* sources cited *supra* notes 18–19.

explains how they would function, and discusses their relative advantages and disadvantages.

A. Removing the Knowledge Inquiry

Knowledge has played a fundamental role in determining Fourth Amendment scope for decades. It has become even more important in recent years as courts are increasingly faced with novel questions posed by new surveillance practices and technologies. Yet courts would do well to reverse this trend and to stop assessing societal knowledge altogether when deciding Fourth Amendment cases. Although relying on societal knowledge helps courts concretize the amorphous inquiry into reasonable expectations and decide Fourth Amendment issues in relatively broad strokes, the fundamental flaws of the knowledge inquiry overwhelm any benefits.

Societal knowledge is a complex, multilayered concept that does not lend itself to easy application in criminal cases. Knowledge typically spreads unevenly through the population, and attributing median societal knowledge to criminal defendants raises questions of fundamental fairness.[290] Judges are societal elites who are systematically likely to overestimate the extent of societal knowledge. Empirical evidence indicates that they do make serious errors in calculating such knowledge.[291] Further, even if societal knowledge could be measured perfectly, anchoring the Fourth Amendment's scope to it will lead to a gradual erosion of Fourth Amendment protection. As an increasingly intelligent and educated population gains awareness and understanding of new technologies and threats to privacy, expectations of privacy and the sphere of Fourth Amendment protection will naturally shrink. In the meantime, rapid and largely random changes in public awareness will render Fourth Amendment law unstable and unpredictable.[292] These theoretical and practical problems should lead courts to abandon the knowledge inquiry in Fourth Amendment law.

The doctrinal implications of abandoning the knowledge inquiry would be substantial. People's expectations of privacy are substantially dependent on what they know in the present. If courts are to discard the problematic inquiry into societal knowledge, must they also discard *Katz*'s reasonable expectation of privacy test?

---

[290] *See supra* Section III.A.

[291] *See supra* Section III.B.

[292] *See supra* Part IV.

The answer is likely yes, at least insofar as that test directs courts to actually assess people's expectations of privacy. Assessing societal expectations necessarily involves, either explicitly or implicitly, an assessment of societal knowledge.[293] As long as the *Katz* test directs lower courts to determine what people reasonably expect, lower courts are likely to use societal knowledge to gain traction on that difficult inquiry. If the knowledge inquiry must go, then so must the examination of people's expectations of privacy.

The situation is more complicated than that, however, because the reasonable expectation of privacy test is not always applied literally. As Orin Kerr pointed out in a landmark study of Fourth Amendment case law, the Supreme Court sometimes focuses on normative or doctrinal considerations rather than actual expectations of maintaining privacy.[294] Kerr identifies two different normative models in the case law.[295] Cases emphasizing the "policy model" engage in relatively overt balancing of the benefits or harms of allowing police to gather information without a warrant.[296] Cases involving the "private facts model" focus on just one normative consideration: the intimate (or non-intimate) nature of the information sought by the government.[297] Kerr also identifies a doctrinal approach called the "positive law model," which finds a privacy violation if the government's action violates a law other than the Fourth Amendment itself.[298]

These nonexpectation models have been criticized as inconsistent with *Katz*'s binding precedent.[299] They may also play less of a role than appearances suggest. Courts often employ multiple approaches to justify their decisions, and in many cases the models described above may yield the same outcome as a more literal application of *Katz*.[300] The expectation model likely remains the dominant approach in Fourth Amendment law.[301]

---

[293] *See supra* Sections II.A–II.C.

[294] Kerr, *supra* note 19, at 505–06.

[295] *Id.* at 524.

[296] *Id.* at 519–20 (noting that in *Kyllo v. United States*, 533 U.S. 27, 40 (2001), for example, the Court expressly took "the long view" and made a normative choice about the appropriate level of privacy in the home).

[297] *Id.* at 512–13 (citing *Dow Chemical Co. v. United States*, 476 U.S. 227, 238 (1986), for instance, in which the Court held that aerial photographs of a chemical plant were not a Fourth Amendment search because they did not reveal anything important or intimate).

[298] *Id.* at 516.

[299] *See, e.g.*, Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1601 & n.67 (2010).

[300] *See* Kerr, *supra* note 19, at 524.

[301] *See* Simmons, *supra* note 125, at 586 n.108.

But the Court's prior use of other models of Fourth Amendment scope may provide a basis for a new test that avoids the current regime's increasingly untenable reliance on societal knowledge. By developing the nascent theories of privacy hinted at in the Court's references to positive law or normative considerations, we can begin to fashion a Fourth Amendment test capable of preserving privacy in the technological age.

The following Sections discuss how this test might be developed. These Sections set out some alternative approaches to determining the Fourth Amendment's scope and explain how these regimes would operate. Again, these relatively short Sections do not offer a comprehensive argument in favor of these alternatives. Rather, they give an overview of the proposed models and examine their various strengths and weaknesses, highlighting the key tradeoffs among the various Fourth Amendment regimes.

B. The Fourth Amendment as a Reflection of Positive Law

In Fourth Amendment cases, the Supreme Court has often used non-Fourth Amendment sources of law to help it analyze reasonable expectations of privacy. The underlying principle of these cases is that the law itself is a reflection of people's reasonable expectations. That is, if the government broke some law in order to obtain information, then it has probably violated people's expectations of privacy. But this principle is not universal.[302] Nor is it necessary to break the law in order to violate the Fourth Amendment.[303]

The Court could take a different path. It could instead develop a test that looks *exclusively* to positive law in determining the scope of the Fourth Amendment. Under this regime, the absence of a law or common law tort prohibiting some government information-gathering activity would definitively establish that the activity was not a search under the Fourth Amendment. The reverse would also apply—when a government investigative action violated positive law, it would constitute a per se Fourth Amendment search.[304]

---

[302] *See, e.g.*, Oliver v. United States, 466 U.S. 170, 183–84 (1984) (holding that police officers who violated trespass law did not violate the Fourth Amendment).

[303] The Court has often held that surveillance activity that breaks no other law nonetheless violates the Fourth Amendment. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001); Bond v. United States, 529 U.S. 334, 338–39 (2000); Arizona v. Hicks, 480 U.S. 321, 324–25 (1987).

[304] This would require revising some existing doctrines. For instance, under current law, police encroachments on privately owned open fields are not considered searches under the Fourth Amendment despite clearly violating trespass law. *See, e.g.*, *Oliver*, 466 U.S. at 183–84.

The core concept of a positive law approach would be that police officers do not "search" under the Fourth Amendment if they have acted lawfully and committed no tort or property violation. This concept finds some support in the Supreme Court's recent trespass-focused cases[305] and recent scholarship advocating that government investigations be regulated by state laws,[306] or that government officials be bound by positive law *and* prohibited from lawfully using government authority to gather information unless they have a warrant.[307] These variations each have their own unique advantages and disadvantages, but in the interests of clarity and brevity this Section will evaluate only its own proposal: a Fourth Amendment regime where only government actions that violate some law or legal duty constitute a Fourth Amendment search.

Such a regime would have some major advantages over the current expectation-based test. The risk that the Fourth Amendment might shrink as knowledge grows would be largely eliminated. Although existing laws would occasionally change, overall stability would likely increase, especially since many of the relevant property and tort concepts have been around for centuries. A positive law regime would also likely increase predictability for both citizens and police. Rather than having to guess at how courts will assess expectations or calculate societal knowledge, these actors could look to legal codes or the law of trespass to determine the extent of Fourth Amendment protections.

However, such a regime would present a number of challenges. For one, the positive law inquiry might be difficult in novel surveillance contexts presenting unresolved legal issues. Such issues may arise

---

[305] *See* Florida v. Jardines, 133 S. Ct. 1409, 1415–17 (2013); United States v. Jones, 132 S. Ct. 945, 949–50 (2012).

[306] Michael J. Zydney Mannheimer, *The Contingent Fourth Amendment*, 64 EMORY L.J. 1229, 1284–87 (2015); Laurent Sacharoff, *Constitutional Trespass*, 81 TENN. L. REV. 877 (2014). Mannheimer argues that citizens' rights against unreasonable searches and seizures are largely contingent on state laws regulating police behavior and that such an approach is most consistent with the views of the primary proponents of the Bill of Rights. Mannheimer, *supra*, at 1285–86. Sacharoff proposes a trespass-based Fourth Amendment test that tracks state laws and is inspired by the *Jones* and *Jardines* cases. Sacharoff, *supra*.

[307] William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV 1821 (2016). Baude and Stern argue, on historical and other grounds, that the Fourth Amendment's "reasonableness" requirement should attach whenever a government actor violates positive law or uses government authority to obtain information. *Id.* at 1831–32. This "nonexceptionalis[t]" positive law model leans less heavily on legislatures, likely providing more privacy protection overall but enjoying fewer of the advantages of legislative control, such as clarity, predictability, and greater institutional competence. *See id.* at 1850–54. It also likely offers more protection for information held by third parties, although it does so at the cost of making Fourth Amendment protection more arbitrary—third-party privacy would largely depend on the efficacy of the government's use of informal pressures to persuade ISPs and telephone companies to share data. *See id.* at 1873–74.

frequently in Fourth Amendment cases, because defendants would likely assert trespass, privacy tort, and statutory claims against police officers in situations that would rarely, if ever, generate litigation between private citizens.[308] Thus a positive law regime, although likely more predictable than the *Katz* test, may still be unpredictable in many cases—especially those involving new technologies or investigative actions rarely taken by civilians.

A positive law rule may also raise concerns about legislation designed to undermine core Fourth Amendment protections for privacy in citizens' homes or belongings.[309] Such concerns might be addressed at least in part by allowing courts to strike down laws that undermine traditional, property-based Fourth Amendment safeguards. For example, if Congress were to pass legislation making it lawful for anyone to encroach on the curtilage of a home, courts might strike it down (as applied to the police) on the basis that it would undermine longstanding, property-based Fourth Amendment protections. This exception to the positive law rule could allow courts to protect a substantial core of Fourth Amendment protection from governmental intrusion without undermining the general structure of a positive law regime. Of course, even a narrow exception would somewhat diminish the predictability of the positive law approach.

The transition to a positive law regime may also be difficult, because such an approach would be substantially underprotective at first. There are likely several areas where privacy-protecting legislation was considered unnecessary because courts had already regulated police behavior under the Fourth Amendment. However, if courts adopted a positive law rule, leaving privacy protection in the hands of Congress and state legislatures, those bodies would presumably respond with some additional privacy-protecting laws.[310]

Accordingly, a positive law regime would carry with it the benefits and costs of enhanced legislative control over criminal procedure. Several scholars have argued in favor of a greater role for legislatures in regulating

---

[308] In both of the recent cases that the Supreme Court resolved on the basis that the police committed a trespass, the trespass question was novel and difficult to resolve. *See Jardines*, 133 S. Ct. at 1422–24 (Alito, J., dissenting) (asserting that a police officer did not commit trespass by walking to a home's front door accompanied by a drug-sniffing dog and noting the absence of precedent on the issue); *Jones*, 132 S. Ct. at 957–58 & n.2 (Alito, J., concurring in the judgment) (contending that attaching a GPS tracker to a car is not a trespass to chattels under current law and may not have been under the common law of 1791).

[309] *See* Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 330–31 (2016).

[310] *See* William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 781, 792–802 (2006) (describing the political forces that would likely motivate criminal procedure legislation in the absence of court-driven regulation).

police behavior.[311] Legislators may have informational advantages over courts, as legislators are able to solicit input from a variety of sources and to revise and amend draft bills before they become law.[312] Legislatures are capable of comprehensive, forward-looking regulation of an entire area, rather than the case-by-case lawmaking that is typical of courts.[313] Legislatures are also better suited to enacting structural reforms that can identify and prevent police misconduct rather than relying on the uncertain *ex post* deterrence of the exclusionary rule.[314]

On the other hand, a Fourth Amendment test that relies on legislative action to address novel surveillance issues may systematically underprotect privacy. Because of the substantial enactment costs of legislation and the preferences of entrenched interest groups, there is a powerful bias in favor of the legislative status quo[315]—which in the privacy context would be the lack of statutory regulation of surveillance. Legislative status quo bias may also be increasing over time. At the federal level, for instance, passing legislation has become more difficult as Congress grows more polarized and the use of filibusters becomes routine.[316] This latter effect may be mitigated somewhat by the fact that political support for privacy protection can be found among both liberals and libertarian-leaning conservatives, increasing the relative likelihood of bipartisan legislation. State legislatures may also be able to fill many of the gaps created by federal gridlock, especially in states with governments dominated by a single party.[317]

Legislative sclerosis is a particular concern in the Fourth Amendment context because of the difficulty of addressing technological change under a positive law regime. New technologies can enable the police to invade personal privacy without violating property or other laws.[318] Moreover, statutes governing communications and other technologies tend to become obsolete fairly quickly, and Congress has historically failed to amend such

---

[311] *Id.*; Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CALIF. L. REV. 205 (2015).

[312] *E.g.*, Kerr, *supra* note 311, at 881.

[313] *E.g.*, *id.* at 868–70.

[314] Rappaport, *supra* note 311, at 239–40.

[315] *See, e.g.*, FRANK R. BAUMGARTNER ET AL., LOBBYING AND POLICY CHANGE: WHO WINS, WHO LOSES, AND WHY 24–26, 45 (2009).

[316] *See, e.g.*, Jody Freeman & David B. Spence, *Old Statutes, New Problems*, 163 U. PA. L. REV. 1, 14 (2014).

[317] *See* Rappaport, *supra* note 311, at 236, 253.

[318] Kerr, *supra* note 19, at 533–34.

laws quickly enough to keep up with technological change.[319] The likelihood of legislatures effectively regulating privacy is diminished when they must enact major amendments to each relevant law every few years to keep pace with new technologies.

There are other substantial downsides to a positive law regime of Fourth Amendment scope. The protection that non-Fourth Amendment laws offer may often be arbitrary, because such laws are enacted for a wide range of reasons that may have nothing to do with privacy.[320] Basing the Fourth Amendment on property concepts or trespass law can also lead to absurd results. For example, in the pre-*Katz* era, the Court held in separate cases that police violated the Fourth Amendment when they used a microphone that touched a heating duct in a suspect's house,[321] but did not violate the Fourth Amendment when they used a microphone that did not physically encroach on a suspect's property.[322] It is the eavesdropping on private conversations, rather than the touching of a heating duct, that invades a person's privacy and raises concerns about government oppression—but under a positive law regime, only the physical touching matters. This is not an inevitable feature of a positive law approach, however, as legislatures may eventually fill in at least some of the gaps left by a property-based regime.

C. Direct Normative Balancing

In deciding the complex cases that make up most of its docket, the Supreme Court frequently makes normative judgments based on policy considerations.[323] Fourth Amendment cases are no different.[324] But the precise character of the normative inquiry used in some Fourth Amendment cases is difficult to discern. The Court's general approach is simply to identify and balance policy considerations that support expanding or

---

[319] *See* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 768–71 (2005).

[320] Kerr, *supra* note 19, at 533.

[321] Silverman v. United States, 365 U.S. 505, 509 (1961).

[322] Goldman v. United States, 316 U.S. 129, 135 (1942) (citing Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967)).

[323] *See, e.g.*, Ariz. State Legislature v. Ariz. Indep. Redistricting Comm'n, 135 S. Ct. 2652, 2658, 2671–77 (2015) (upholding Arizona's independent congressional redistricting commission based on policy and precedential considerations); Harris v. Quinn, 134 S. Ct. 2618, 2633–34, 2637–38 (2014) (discussing the practical downsides of a longstanding labor law precedent and the policy reasons for refusing to extend it to medical home-care workers).

[324] *See* Kerr, *supra* note 19 at 519–21.

curtailing the Fourth Amendment's scope.[325] Likewise, most of the scholarship on normative approaches to the Fourth Amendment has focused on identifying especially invasive surveillance techniques or noting some of the general circumstances that are relevant to privacy, such as the location and nature of the information sought.[326]

Merely considering the policy implications of Fourth Amendment decisions is not a sufficiently rigorous test for determining Fourth Amendment scope.[327] A more promising approach focuses on explicit normative balancing—weighing the benefits to law enforcement of an information-gathering activity against the harms to citizens. The Supreme Court has provided a doctrinal foundation for such an approach in a case involving prison cell inspections. In *Hudson v. Palmer*, the Court resolved the question whether police could examine a prisoner's cell without probable cause by directly balancing "the interest of society in the security of its penal institutions" against "the interest of the prisoner in privacy within his cell."[328] Because a prisoner's interest in privacy is already greatly compromised, society's interest in safe prisons outweighs it, and suspicionless inspections of prison cells do not violate the Fourth Amendment.[329]

The balance of benefits to law enforcement and harms to privacy arguably goes to the core of the Fourth Amendment inquiry considered in this Article. Unfortunately for our purposes, however, it is not a rigorous or well-elaborated test. It requires each individual court to determine how best to assess privacy harms—a practice that would likely lead to inconsistent conclusions about which aspects of privacy are most valuable. Scholars have established numerous theories of privacy and created large

---

[325] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (reasoning that privacy in houses should be maintained at roughly the same level that it was prior to the invention of thermal imagers); Delaware v. Prouse, 440 U.S. 648, 662–63 (1979) (reasoning that the Fourth Amendment's scope would be too small if the government were allowed to search automobiles without suspicion).

[326] *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 60–70 (listing characteristics of invasive techniques); 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, 985–1014 (2007) (noting several nondispositive factors relevant to privacy); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 722–23 (1988) (listing factors relevant to privacy).

[327] *See* Ohm, *supra* note 130, at 1312 (criticizing existing normative approaches on similar grounds).

[328] 468 U.S. 517, 527 (1984).

[329] *Id.* at 527–28 (first citing Lanza v. New York, 370 U.S. 139, 143–44 (1962); and then citing Bell v. Wolfish, 441 U.S. 520, 537 (1979)).

taxonomies of privacy harms.[330] There are also harms to citizens that cannot be classified as privacy harms but are nonetheless relevant to the Fourth Amendment balance, such as psychological trauma resulting from police coercion or the threat of force.[331] Asking courts to consider each potential harm would result in indeterminacy and prohibitively high decision costs.

Courts could, however, develop a more concrete direct balancing test. I propose one such test below, the aim of which is to incorporate essential categories of law enforcement benefits and citizen harms, while remaining concise and workable for judges. This is certainly not the only feasible balancing test imaginable, and I invite others to propose modifications and alternatives, keeping the goals of comprehensiveness and workability in mind. What follows is a brief overview of the proposed test and an analysis of its primary strengths and weaknesses.

1. An Elaborated Balancing Test.—A direct normative balancing test would find a Fourth Amendment search when the harms to citizens of allowing police to engage in a certain type of surveillance without a warrant outweigh the benefits to society via improved law enforcement. The facts of the case would define the type of surveillance at issue, but the assessment would consider the benefits and costs of allowing the police to conduct such warrantless surveillance in general.[332] This inquiry would align courts' assessments with the potential consequences of their Fourth Amendment decisions. After all, when a court decides that the police may dig through one individual's trash bags without a warrant, the police can then lawfully dig through the trash bags of any citizen in the court's jurisdiction.[333]

---

[330] *See, e.g.*, SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION (1983); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[331] William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1065–66 (1995).

[332] For a less fact-based approach to determining when to apply the Fourth Amendment, see David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 101–03 (2013) (advocating for Fourth Amendment rulings that would apply to all uses of a given technology).

[333] *See* California v. Greenwood, 486 U.S. 35, 40 (1988). Of course, resource constraints are likely to prevent police departments from examining the trash of every citizen in a jurisdiction. For different types of surveillance or for national security matters, however, the government might actually surveil most or all citizens. Courts applying a normative test would primarily focus on the domestic law enforcement context but could also consider the domestic security context if doing so is helpful. By contrast, foreign intelligence surveillance may be exempt from the warrant requirement in any event, making the question whether such surveillance is a "search" largely irrelevant. *See generally* United States v. Truong Dinh Hung, 629 F.2d 908, 913–15 (4th Cir. 1980) (discussing the various reasons that "the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance," but noting that those reasons do not justify warrantless domestic surveillance).

I briefly describe the factors of my proposed test below, starting with the benefits to the law enforcement side of the balance. These benefits can be elaborated as two factors: the usefulness of surveillance conducted without a warrant in detecting crime, and the cost of substituting less invasive forms of surveillance. The first factor essentially asks, how valuable to law enforcement would it be to be able to engage in this type of surveillance without a warrant? Thus, a court might consider whether a surveillance technique would primarily be used in the early stages of investigations, before probable cause has been developed, and whether the warrantless use of the technique would be likely to reveal criminal activity that would otherwise go undetected.[334] For example, if obtaining certain financial records without a warrant would allow police to identify white-collar crimes that would otherwise be difficult to detect, that would weigh in favor of excluding such records from Fourth Amendment regulation.[335]

The second factor asks: is there a less invasive practice that could reveal roughly the same information, and if so how costly would it be for police to use that practice instead? If a surveillance technique is invasive or affects an entire population, and an alternative approach could obtain the same information in a less invasive or more targeted way, that would weigh in favor of applying the warrant requirement of the Fourth Amendment to such surveillance. Courts currently ask a similar question in cases involving the Wiretap Act, which directs the government to show that it has attempted other, less invasive investigative procedures before applying for a wiretap.[336]

On the other side of the balance, the harms to citizens can be elaborated as three factors: the societal costs of people avoiding certain activities because of fear of surveillance; the harm to interpersonal relationships caused by observation; and psychological harm suffered due

---

[334] Courts could also consider relevant studies examining the effects of limiting various surveillance techniques. One recent study, for instance, found that subjecting telephone call logs to a warrant requirement resulted in fewer applications for wiretaps and a decrease in the duration of permitted wiretaps. Anne E. Boustead, *Does Rejection of the Third Party Doctrine Change Use of Electronic Surveillance? Evidence from the Wiretap Reports* (manuscript at 21–24), http://www.rand.org/content/dam/rand/pubs/rgs_dissertations/RGSD300/RGSD384/RAND_RGSD384.pdf [https://perma.cc/7ZKQ-98JA] (on file with author). Its findings suggest that regulating the acquisition of call log data reduces police officers' ability to obtain sufficient probable cause for Wiretap Act applications. *Id.*

[335] *See* Kerr, *supra* note 47, at 509 (explaining that the Supreme Court eliminated the warrant requirement for financial records following the rise of difficult-to-detect white-collar crimes); *see also* David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 777–78, 798 (2013) (discussing types of digital evidence that are especially helpful in detecting healthcare fraud and cyberharassment).

[336] *See* 18 U.S.C. § 2518(1)(c) (2012); United States v. Carter, 449 F.3d 1287, 1293 (D.C. Cir. 2006).

to surveillance or investigation. The first factor asks, if a surveillance technique hypothetically became widespread and well-known, would people avoid socially beneficial activities and, if so, how costly would that be? People engage in all manner of potentially embarrassing or controversial activities, such as visiting a psychiatrist, purchasing certain drugs or medical equipment, researching sensitive subjects online, or criticizing government or social elites. These socially beneficial activities can be deterred by the threat of surveillance.[337] For example, Google searches for terms deemed by user surveys as especially controversial or embarrassing decreased significantly following Edward Snowden's disclosure of an NSA program capable of capturing internet information.[338] If a surveillance practice is likely to cause such chilling effects, that would weigh in favor of Fourth Amendment protection.[339]

The second factor asks whether a surveillance practice would harm interpersonal relationships by compromising intimate communications, preventing the formation of relationships, or reducing the quality or depth of intimate relationships via the threat of observation. Intimate relationships are extremely important to people's well-being and particularly dependent on privacy to flourish.[340] The impact of outside surveillance on relationships is also likely to be relatively easy for judges to intuit, once they endeavor to assess it. If, for instance, a surveillance technique is likely to interfere with personal communications enough to prevent people from expressing private, provocative, or intimate thoughts to each other,[341] that would weigh in favor of finding a Fourth Amendment search.

---

[337] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1129–32 (2002) (discussing the importance of privacy to many personal and group practices).

[338] Alex Marthews & Catherine Tucker, Government Surveillance and Internet Search Behavior (April 29, 2015) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564&download=yes [https://perma.cc/CFV9-GMNK]. Search terms studied included "abortion," "gender reassignment," "police brutality," and "tax avoidance." *Id.* at 35–37.

[339] The costs of defending oneself against surveillance in order to engage in beneficial activities would also be relevant to the analysis of this factor. *See generally* Simmons, *supra* note 125, at 558 (discussing the defensive costs of privacy protection). For example, if internet users are likely to purchase and use sophisticated encryption software in order to mitigate government surveillance, the costs of doing so would be added to the avoidance cost calculus. Defensive expenditures are likely to be relatively small, however, because effective defenses against government surveillance are likely to be unavailable or prohibitively costly. *See supra* notes 187–89.

[340] *See, e.g.*, Strahilevitz, *supra* note 19, at 923–24.

[341] *See* Carl Botan, *Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects*, 63 COMM. MONOGRAPHS 293, 307, 309–10 (1996) (finding that workers under surveillance engaged in fewer personal communications).

Finally, the third factor asks whether, even in the absence of tangible effects on activities or relationships, people will suffer psychological harm as a result of surveillance or investigation. This inquiry would preferably focus on the concrete harms demonstrated in psychological studies,[342] but it could also incorporate more theoretical claims about privacy and personality development.[343] That said, most judges would likely not research surveillance and psychological harm themselves, but would rely on the submissions of parties in litigated cases—much as judges and juries examine the parties' arguments in personal injury cases and assess damages for psychological pain and suffering.[344] Under this factor, evidence that a surveillance technique will likely cause stress, decreased motivation, or feelings of infantilization in the people observed[345] would weigh in favor of Fourth Amendment protection.

If, considering these factors, the total harm to citizens from warrantless surveillance outweighs the total benefit from enhanced law enforcement, courts should hold that the Fourth Amendment requires police to obtain a warrant before conducting the surveillance. Conversely, if the benefit to law enforcement outweighs the privacy harm, then the police should be able to conduct the surveillance without Fourth Amendment regulation.

2. Evaluating the Direct Normative Approach.—The factors identified above are intended to be both concrete and pragmatic. They direct courts' attention to the core policy considerations of the Fourth Amendment inquiry but do not require courts to establish any particular definition of privacy. Of course, courts can and should consider other sources of information in answering the questions raised by the direct

---

[342] *See, e.g.*, *id.* at 307–10; John R. Aiello & Kathryn J. Kolb, *Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress*, 80 J. APPLIED PSYCH. 339, 339–40 (1995); *see also* Stuntz, *supra* note 331, at 1065–66 (discussing psychological harm arising from police coercion).

[343] *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000).

[344] *See* Sean Hannon Williams, *Self-Altering Injury: The Hidden Harms of Hedonic Adaptation*, 96 CORNELL L. REV. 535, 543–44 & n.42 (2011) (collecting cases involving hedonic damages). In fact, the inquiry would be substantially easier, as the psychological harm from surveillance need only be situated somewhere on the general scale from low to high and would not have to be translated into a precise money value. Fact finders tend to be far more consistent in performing the former calculation than the latter. Cass R. Sunstein et al., *Assessing Punitive Damages (with Notes on Cognition and Valuation in Law)*, 107 YALE L.J. 2071, 2097–2103 & tbl.1 (1998) (finding that mock jurors assessing various hypothetical cases tend to give consistent rankings of blameworthiness but very different damages awards).

[345] *See* Botan, *supra* note 341, at 309; Carl Botan & Mihaela Vorvoreanu, *"What Are You Really Saying to Me?" Electronic Surveillance in the Workplace*, CERIAS TECH REPORT, June 2000, at 9–10, http://www.antoniocasella.eu/nume/Botan_2000.pdf [https://perma.cc/NW9G-MPBN] (paper originally presented at the *Conference of the International Communication Association* in Acapulco, Mexico).

balancing test. For example, survey information about how invasive people consider various surveillance techniques may be helpful, as might the identification of well-defined social norms relevant to privacy.[346] But ultimately this normative approach is distinguished by its directness. It calls for courts to address the central normative balance underlying Fourth Amendment jurisprudence, rather than a proxy consideration (like expectations of privacy) that does not fully capture that balance.[347]

This Section discusses some strengths and weaknesses of a direct normative approach to determining Fourth Amendment scope. Such a regime would have substantial advantages over other existing or potential tests. As mentioned above, a court's Fourth Amendment holding in a given case will determine the legality of similar instances of surveillance and affect the behavior of all government entities and potentially all citizens in the court's jurisdiction.[348] A normative approach would allow courts to consider these implications directly, potentially producing better decisions than a regime based on proxy doctrines like the *Katz* test or a positive law standard. Relatedly, the approach would focus on the normative core of the Fourth Amendment inquiry and directly analyze societal costs and benefits. If judges administer it effectively, then its outcomes should maximize societal welfare. In practice, however, judges may be unable to apply the test effectively, as I discuss further below.

One benefit of a direct approach is that it would better harmonize theory and practice. To the extent that the Supreme Court is already deciding cases based on normative considerations while purporting to rely on assessments of societal knowledge,[349] a normative approach would align the Court's opinions with the considerations actually driving its decisions. Supreme Court cases directing courts to look to societal knowledge or other problematic metrics can cause significant harm even if the Court's decisions are primarily driven by policy considerations.[350] Not only are

---

[346] *See, e.g.*, 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(d), at 587–90 (5th ed. 2012); Slobogin & Schumacher, *supra* note 219, at 737.

[347] *See* Kerr, *supra* note 19, at 536 (noting that the policy model of Fourth Amendment law addresses "the basic goal of the reasonable expectation of privacy test, which must identify police practices that are reasonable per se and separate them out from more invasive police practices that could only be reasonable in some specific contexts").

[348] Exceptions to this general rule can be imagined, but typically, a court's ruling on the constitutionality of a type of surveillance will be determinative in cases involving the same surveillance technique.

[349] *See* Kerr, *supra* note 19, at 519, 522 (suggesting that normative considerations likely drive outcomes in Supreme Court Fourth Amendment cases even when the opinion focuses on expectations of privacy or positive law).

[350] *See, e.g.*, RICHARD A. POSNER, HOW JUDGES THINK 269–72 (2008) (arguing that the Supreme Court is an inherently political court).

lower courts likely to follow the doctrines set out by the Supreme Court,[351] but the Court itself may feel compelled to follow the same doctrines in subsequent cases regardless of whether those doctrines produce undesirable outcomes.[352]

A direct normative approach would also be resilient to societal change and in little danger of shrinking as knowledge of privacy threats increases. It would be better suited than a positive law regime to addressing new surveillance technologies, as it would not require new legislation to address novel privacy issues.[353] This adaptability may be especially important given the outsized role that technological change plays in Fourth Amendment law.[354]

Finally, the normative approach would allow courts to consider the psychological effects of police practices that infringe upon Fourth Amendment values other than privacy. In many law enforcement contexts, such as stop-and-frisk encounters or vehicle stops, police coercion and the threat of force cause citizens more psychological harm than the concomitant privacy violations.[355] These harms may be exacerbated if the surveillance at issue has been carried out in a discriminatory or non-investigatory manner.[356] The *Katz* test's focus on expectations of privacy leaves little room for weighing these substantial harms.

One of the disadvantages of a direct normative test would be its complexity relative to other potential tests. Multifactor tests generally impose higher decision costs per case than simpler tests.[357] A Fourth Amendment normative test also asks judges to consider the future effects of their decisions on police and citizen behavior, a policy inquiry that is arguably better suited to a legislature.[358] Of course, judges are hardly inexperienced in considering the policy implications of their decisions.

---

[351] Kerr, *supra* note 19, at 545–46; Tokson, *supra* note 173, at 908.

[352] *See, e.g.*, Allied-Bruce Terminix Cos., Inc. v. Dobson, 513 U.S. 265, 283 (1995) (O'Connor, J., concurring) (voting to reverse but noting, "[w]ere we writing on a clean slate, I would [vote to] affirm"); Flood v. Kuhn, 407 U.S. 258, 279–82 (1972) (upholding an arguably "unrealistic, inconsistent, or illogical" ruling regarding baseball's antitrust status because "the aberration is an established one") (citing Radovich v. Nat'l Football League, 352 U.S. 445, 452 (1957) (noting that the rule is undesirable but well established)).

[353] *See supra* notes 315–19 and accompanying text.

[354] *See* Kerr, *supra* note 47, at 528.

[355] Stuntz, *supra* note 331, at 1065–66.

[356] *See, e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540, 561 (S.D.N.Y. 2013).

[357] Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 572–86 (1992).

[358] Legislatures tend to take a broader view of policy issues and to consider future consequences. Courts more typically decide cases on the basis of past events or by addressing particular circumstances. *See, e.g.*, Kerr, *supra* note 311, at 868.

When faced with a question of first impression, especially one not easily resolved by reference to existing laws or precedents, courts often expressly consider the policy implications of their potential rulings.[359] Moreover, even in cases purportedly decided based on formal doctrinal interpretations, judges' decisions are often driven by underlying policy considerations.[360] Accordingly, litigants have been presenting "Brandeis briefs" focusing on policy arguments and empirical data since well before Louis Brandeis filed his famous brief in *Muller v. Oregon* in 1908.[361] The use of general, policy-relevant facts by courts has continued and possibly accelerated in the internet age, and can be observed in state as well as federal courts.[362] None of this is to say that courts are as well suited to forward-looking policy judgment as legislatures are. They are, however, capable of such judgment and exercise it more than occasionally.

Another concern is that a normative regime would also give judges a great deal of discretion in setting the boundaries of Fourth Amendment protection. Judicial assessments of costs and benefits might vary widely, especially among judges with different policy preferences or attitudes about privacy. However, the discretion granted by the normative test may not ultimately differ much from that granted by the reasonable expectation of privacy test. Judges' assessments of knowledge and expectation may be strongly influenced by their preferences and biases,[363] and the largely nonempirical nature of the knowledge inquiry gives judges a great deal of discretion in dictating case outcomes.

A related objection to policy-focused Fourth Amendment regimes in general is that they would be unpredictable and inconsistent across cases.[364] This lack of predictability is also problematic because the Fourth Amendment regulates police behavior, and the police may have difficulty predicting what is lawful under a normative regime.[365] These drawbacks are

---

[359] This occurs frequently in the Fourth Amendment context, *see, e.g.*, Arizona v. Gant, 556 U.S. 332, 344–46 (2009); Hudson v. Palmer, 468 U.S. 517, 526–28 (1984), and in other contexts, *see, e.g.*, Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 452–54 (1984); United States *ex rel.* Martin v. Life Care Centers. of America, Inc., 114 F. Supp. 3d 549, 571–72 (E.D. Tenn. 2014); *In re* Rose, 512 B.R. 790, 796 (Bankr. W.D.N.C. 2014); Rothrock v. Rothrock Motor Sales, Inc., 810 A.2d 114, 117 (Pa. Super. Ct. 2002).

[360] *See, e.g.*, Kerr, *supra* note 19, at 519, 522; POSNER, *supra* note 350, at 111, 118–19.

[361] *See* Noga Morag-Levine, *Facts, Formalism, and the Brandeis Brief: The Origins of a Myth*, 2013 U. ILL. L. REV. 59, 71–72 (discussing how judicial reliance on "legislative facts" about public health predates Brandeis's famous brief).

[362] *See* Cathy Cochran, *Surfing the Web for a "Brandeis Brief": The Internet and Judicial Use of Legislative Facts*, 70 TEX. B.J. 780, 780–82 (2007).

[363] *See supra* Section III.B.2.

[364] *E.g.*, Kerr, *supra* note 19, at 536.

[365] *See* Amsterdam, *supra* note 42, at 403–04.

significant, but a normative regime would probably not be any more unpredictable than the current system of Fourth Amendment law, where courts focus on one of several models of the *Katz* test more or less at random.[366] Even the positive law regime may be unpredictable when faced with new legal issues.[367]

In most situations, under any test, police will simply look to settled law on the constitutionality of various investigation activities. An officer need not conduct a fresh Fourth Amendment inquiry to know that he needs a warrant to search a house, tap a phone, open a sealed letter, look through a footlocker, or examine a cell phone's contents. Novel situations, by contrast, may be difficult for police officers to resolve no matter how the Fourth Amendment's scope is determined.

A normative standard may also become more rule-like and predictable over time. As courts flesh out the normative test and determine the constitutionality of various types of activity, future applications of the test will become more predictable.[368] That said, the outcomes of a multifactor test would be less certain than a rule-based regime. Thus the positive law approach, whatever its other drawbacks, would likely perform best in terms of predictability and consistency across decisions.

Both of these alternatives would be more resilient to social and technological change and the expansion of societal knowledge than the current regime. They would be no less predictable than the multimodel *Katz* approach. And both would avoid the conceptual and practical problems at the core of a knowledge-based test.

CONCLUSION

Courts rely heavily on societal knowledge to determine the Fourth Amendment's scope. In part, this reliance is compelled by the *Katz* test—what people know generally dictates their reasonable expectations of privacy. But courts' reliance is also driven by the relative ease of making intuitive judgments about societal knowledge. Rather than considering the questions at the core of the Fourth Amendment—questions about the harms of oppressive surveillance and the benefits of unfettered police investigations—courts can simply decide whether people knew their privacy was compromised.

Yet, as this Article has shown, there are substantial conceptual problems inherent in the assessment of societal knowledge. Knowledge is

---

366 *See* Kerr, *supra* note 19, at 507–25.

367 *See supra* note 308 and accompanying text.

368 *See* Michael Coenen, *Rules Against Rulification*, 124 YALE L.J. 644, 654–55 (2014).

not a simple binary; it is a complex, multiphase process. It spreads unevenly throughout the population and may never reach people with lower levels of social status, education, or wealth. Moreover, people may remain ignorant of widely available knowledge because they fail to process information that challenges their beliefs or rationally avoid learning information for which they have little use. Marshaling existing studies of user knowledge and original survey data, this Article has demonstrated how these problems result in empirical errors in Fourth Amendment cases.

This Article has also examined whether, even if societal knowledge could be measured perfectly, courts should nonetheless abandon its use as a determinant of the Fourth Amendment's scope. Demographic data strongly suggests that future generations will be more intelligent, better educated, and far more knowledgeable about technology than the current population. A knowledge-based Fourth Amendment is likely to shrink over time as society becomes better informed about new technologies and threats to privacy. In the interim, societal knowledge will be unpredictable and unstable, prone to sudden spikes in awareness following high-salience news stories or government leaks. This Article has outlined some alternative approaches likely to be more coherent and more durable than the current model. Going forward, Fourth Amendment law might embrace privacy protection dictated by traditional property concepts and by Congress, or it might look more directly at the normative balance underlying the concept of a Fourth Amendment search. These approaches have their own disadvantages, but either would avoid the central danger of the current approach—a Fourth Amendment of ever-declining relevance to government surveillance and citizens' privacy.