REASONABLE EXPECTATIONS OF ANONYMITY

Jeffrey M. Skopek[*]

INTRODUCTION

NEW technologies and methods of data analysis are being used by the government to monitor the public in ways that were unimaginable a decade ago. Law enforcement agencies ranging from municipal police forces to the Department of Homeland Security are using tools such

[*] University of Cambridge Faculty of Law. Thanks to David Barron, Yochai Benkler, John Coates, Glenn Cohen, John Goldberg, Matt Lawrence, Nicholson Price, Chris Robertson, Todd Rakoff, Joe Singer, Holger Spamann, Carol Steiker, Matthew Stephenson, Larry Tribe, Mark Wu, and workshop participants at Harvard Law School, the University of Cambridge Faculty of Law, and the New England Regional Junior Faculty Workshop for helpful conversations and comments. This work was made possible by a fellowship from Harvard Law School's Petrie-Flom Center.

as genetic databanks,[1] biometric scanners,[2] roadside cameras,[3] and cell phone metadata analysis[4] to gather detailed information about the lives of individuals who are not suspected of any wrongdoing. The meaningful question in this area is no longer what information the government can obtain about us, but rather what information is beyond its reach.

The reason for this is that the Supreme Court has concluded that the Fourth Amendment's protections do not apply to any information that has been exposed to the public or third parties. This includes information about our public movements, Internet usage, cell phone calls, and so on. Such information is per se fair game for police collection by any means.

This Article argues that the Court's conclusion derives from a mistaken conflation of privacy and anonymity, and that understanding the difference between these concepts reveals strong substantive and formal reasons for interpreting the Fourth Amendment to protect not only reasonable expectations of privacy, but also "reasonable expectations of anonymity." Further, it demonstrates that the incorporation of this new analytic concept into Fourth Amendment jurisprudence yields significant value: first, by identifying otherwise-unrecognizable ways in which new techniques of big data implicate the Constitution, and second, by delivering on the unfulfilled promise of the Supreme Court's teaching that "the Fourth Amendment protects people, not places."[5] A more detailed roadmap of this argument follows.

---

[1] The police in nearly every state and the FBI are creating genetic profile databases. Rich Williams, Forensic Science Database: Search by Policy, Nat'l Conf. State Legislatures (Aug. 5, 2014), http://www.ncsl.org/research/civil-and-criminal-justice/dna-database-search-by-policy.aspx#5. Originally, only those convicted of felonies were required to submit DNA samples, but the federal government and most states now require profiling of arrestees as well. Id.; see also 28 C.F.R. § 28.12(b) (2012) (requiring federal agencies to collect DNA samples).

[2] See, e.g., Charlie Savage, Facial Scanning Is Making Gains in Surveillance, N.Y. Times, Aug. 21, 2013, at A1 (describing the Department of Homeland Security's Biometric Optical Surveillance System, which will be able to scan crowds in public spaces and automatically identify and track individuals).

[3] See, e.g., ACLU, You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements 2 (July 2013), available at https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record (describing the widespread use of road-side cameras to amass millions of digital records on the location and movement of every vehicle with a license plate).

[4] See, e.g., Richard Lempert, PRISM and Boundless Informant: Is NSA Surveillance a Threat? Brookings (June 13, 2013, 10:31 AM), http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert (describing the NSA's Boundless Informant program, which captured a vast and indiscriminate class of metadata from U.S. citizens' phone calls).

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

The argument begins, in Part I, with an analysis of the Fourth Amendment right to be free from unreasonable "searches"—a term that the Supreme Court has, ever since *Katz v. United States*, interpreted to mean violations of reasonable expectations of privacy. The key contribution of this Part is clarifying what the Court means by "privacy" in the Fourth Amendment context, which has been the subject of much confusion in the literature. A close analysis of the case law reveals that the Court has adopted what can be termed an "epistemic," rather than a normative, conception of privacy. The clarification of this point provides the foundation for a discussion of two doctrines that significantly limit the scope of the Fourth Amendment's protections: the public exposure and third party doctrines, under which the Supreme Court has concluded that the Fourth Amendment's protections do not apply to any information that has been exposed to the public or third parties.

The question that motivates this Article is whether the Supreme Court has erred in reaching this conclusion. The dominant view in the privacy scholarship is that the Court has failed to account for the ways in which privacy can exist in degrees. While this critique is correct as far as it goes, this Article demonstrates that it only identifies part of the problem.

The even deeper problem, identified in Part II, is that courts—along with most scholars—have incorrectly assumed that there is only one way of protecting a piece of personal information from public access: the one we call "privacy." In doing so, they have overlooked a distinct and equally important way of doing so: through anonymity. This oversight derives from the fact that anonymity and privacy have been mistakenly conflated.

An example helps introduce the key distinction that has gone unrecognized. Imagine, for instance, that a person's medical file contains a piece of paper with the results from his blood test, but his doctor removes the paper and places it in a blank file. If we subsequently obtained access to this person's medical file, without the test results, we would describe the situation using the concept of privacy: We would say "the privacy of the person is protected," or "the associated information is private." If, on the other hand, we obtained access to the test results, without the medical file, we would describe the situation using the concept of anonymity: We would say "the anonymity of the test results is protected," or "the associated person is anonymous."

What this example illustrates is two basic points about anonymity and privacy that have been misunderstood. The first is a point about their

substantive difference. Although both anonymity and privacy prevent others from gaining access to a piece of personal information, they do so in opposite ways: Privacy involves hiding the *information*, whereas anonymity involves hiding what makes it *personal*. The second point is about their formal relationship. Anonymity and privacy have the same causal origin and thus are flip sides of each other: They describe opposite sides of a single underlying event.

This account of the nature of anonymity, when combined with the insight that *Katz* and its progeny adopt a purely epistemic conception of privacy, has significant legal implications. As identified in the final Section of Part II, it reveals strong substantive and formal reasons for reading the Fourth Amendment to protect not only reasonable expectations of privacy, but also "reasonable expectations of anonymity."

It is perhaps worth highlighting here that this is not a normative argument about what our constitutional law should be, but rather a legal argument about the best way to interpret the Fourth Amendment precedents that we have. Thus, I do not question whether *Katz* and its progeny provide the best interpretation of the text of the Fourth Amendment, but rather make a claim about the best reading of this case law, accepting that it provides a controlling reading of the text. Further, and relatedly, I do not question the premise that the Fourth Amendment does not prohibit the government from collecting personal information that has been knowingly exposed to the public, but rather show that this premise does not support the conclusions reached by courts in many of the public exposure cases—that the logic of the public exposure doctrine imposes limits that have not been recognized. This is not to say, however, that my argument is at odds with those of scholars who argue for more radical revisions of Fourth Amendment jurisprudence on normative grounds.[6] Rather, a normative approach might reach the same conclusions on many issues, as will become clear in Part III.

The practical payoff of incorporating the concept of "reasonable expectations of anonymity" into Fourth Amendment jurisprudence is the focus of Part III, which identifies two general dimensions in which it yields significant insights. The first dimension is analytic, where thinking in terms of anonymity identifies otherwise-unrecognizable ways in

[6] See, e.g., David Alan Sklansky, Too Much Information: How Not to Think About Privacy and the Fourth Amendment, 102 Calif. L. Rev. 1069, 1113–15 (2014) (arguing that the Fourth Amendment should be interpreted to protect not only informational privacy, but also "zones of personal refuge").

which many new techniques of big data implicate the Fourth Amendment. This is demonstrated by reference to the question of whether two new techniques of data aggregation and analysis can constitute Fourth Amendment searches. One is a form of genetic identification known as "familial searching," in which a criminal DNA database is used to identify persons who do not meet the legal criteria for inclusion, but happen to be related to people who do. The other is the use of tools such as biometric-equipped video cameras, GPS, and the metadata from cell phone calls to conduct long-term locational tracking of people's movements in public.

Both of these techniques have faced significant criticism in the privacy scholarship, and there is language in judicial opinions questioning their legitimacy, but neither the literature nor the judicial opinions have offered a strong legal argument for how they can constitute Fourth Amendment searches. The reason for this is that the constitutional problem cannot be sufficiently explained in terms of privacy.

What is needed is the concept of reasonable expectations of anonymity, which not only reveals the Fourth Amendment interests that are violated by these specific techniques, but also provides a meaningful standard that can be used more generally to determine when data aggregation implicates the Fourth Amendment and when it does not. In these ways, the concept helps solve difficult puzzles left open by the concurring opinions in *United States v. Jones*.[7]

In addition to providing the analytic power necessary to understand the unconstitutionality of many new techniques of big data, the incorporation of anonymity into Fourth Amendment jurisprudence will help deliver on the unfulfilled promise of the Supreme Court's teaching that the Fourth Amendment is meant to protect "people, not places."[8] There are

[7] 132 S. Ct. 945 (2012). Justice Alito explained in concurrence—joined by Justices Ginsburg, Breyer, and Kagan—that he would have held that the twenty-eight-day-long GPS tracking of the defendant's car violated his reasonable expectations of privacy. Id. at 957–64 (Alito, J., concurring). Justice Sotomayor expressed sympathy with this view in her concurrence, but she ultimately joined the Court's narrower holding that placing the GPS on the car violated the Fourth Amendment on the grounds that it involved trespass onto the defendant's private property. Id. at 954–55 (Sotomayor, J., concurring). However, neither concurrence articulated a rule or standard that could be applied in other cases, nor did they explain why public surveillance information is not categorically exempted from Fourth Amendment protection by the public exposure doctrine as most courts and scholars had concluded.

[8] *Katz*, 389 U.S. at 351.

two central ways in which it does so, as the final Section of Part III demonstrates.

The first is by revealing that the structural features of the world that are capable of protecting Fourth Amendment interests are far more complex and expansive than the Supreme Court has recognized. Although the Court has moved beyond a property-based conception of Fourth Amendment interests, the only structural features of the world that the Court has recognized as protecting these interests are those that protect the "privacy" side of secrecy: Homes, car trunks, envelopes, and other containers all hide facts about a person whose identity might be known. Yet the structures that are capable of maintaining the secrecy of "personal information" are not limited to those that hide the piece of *information*. Rather, as this Article makes clear, they can also include structures that hide what makes that information *personal* or, in other words, structures that make it anonymous. For example, the size of a city, the layout of its streets, and the presence of crowds can all contribute to making someone's public actions anonymous. By uncovering the legal significance of these structures, attention to anonymity opens up new types of public spaces to the Fourth Amendment's protections.

The second and related way in which attention to anonymity can help deliver on the promise of the Fourth Amendment is by expanding the sources of law and norms that can provide the basis for its protections. Although property law is often cited as the quintessential enabling source of law for reasonable expectations of privacy, reasonable expectations of anonymity may be created by sources of law ranging from whistle-blowing statutes and agency law to copyright and the First Amendment, all of which protect anonymity rights.[9] In the First Amendment context, for example, the Supreme Court has held that "an author's decision to remain anonymous . . . is an aspect of . . . freedom of speech."[10] Thus, an anonymity-based understanding of Fourth Amendment claims could ground them in new legal and normative foundations, including other constitutionally protected liberties.

[9] See Jeffrey M. Skopek, Anonymity, the Production of Goods, and Institutional Design, 82 Fordham L. Rev. 1751, 1759–62 (2014).

[10] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995). This is just one of many Supreme Court cases to recognize the right. See Chesa Boudin, Publius and the Petition: *Doe v. Reed* and the History of Anonymous Speech, 120 Yale L.J. 2140, 2164–68 (2011) (discussing the many other Supreme Court cases that have recognized an anonymity right in the First Amendment).

Further, these two lessons—along with the other insights of this Article—are not only applicable to the Fourth Amendment. Rather, as suggested in the Conclusion, they are relevant to the many other sources of law that provide legal protection to reasonable expectations of privacy. Across all of these domains, attention to the distinct concept of anonymity can reveal important and viable interests in the secrecy of personal information that have gone unrecognized, clarify new ways in which these interests are being threatened, and provide insights into how they can be better protected by our courts and our law.

I. REASONABLE EXPECTATIONS OF PRIVACY

A. The Fourth Amendment

The Fourth Amendment provides people with the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[11] Thus, the threshold question in Fourth Amendment jurisprudence is whether a particular government action constitutes a search or seizure. If it does, the action must be "reasonable," which means that it must be based on probable cause and carried out pursuant to a warrant (unless it falls within a judicially defined exception to one or both of these requirements). This Article is concerned with the preliminary question of whether government conduct constitutes a constitutional "search," which the Supreme Court has defined with two tests.

The first test—which was in place from the Founding until 1967, when it was seemingly rejected by the Court but which the Court has just reaffirmed—is based in property law.[12] Under this test, a search consists of a physical trespass to one of the constitutionally specified zones (namely, "persons, houses, papers, and effects") with the intent to collect information.[13] A paradigmatic example of this approach is the wiretapping case of *Olmstead v. United States*, in which the police inserted small wires into the telephone lines outside the defendants' residences and main office, thereby intercepting conversations that uncovered an illegal conspiracy.[14] Because the insertion of the wires did not

[11] U.S. Const. amend. IV.
[12] See *Jones*, 132 S. Ct. at 949–50.
[13] Id. at 951 n.5.
[14] Olmstead v. United States, 277 U.S. 438 (1928).

require any physical trespass onto the defendants' property, the Court determined that no Fourth Amendment search had occurred.[15]

The second test comes from the Court's attempt—in the 1967 case of *United States v. Katz*[16]—to address the limits of the property-based approach in an era of surveillance technologies that no longer required physical trespass.[17] Returning to the question of the constitutionality of warrantless wiretapping, the Court held that FBI agents had violated the Fourth Amendment when they attached an electronic recording device to the top of two public telephone booths being used by Katz. In rejecting the property-based approach of *Olmstead*, the Court explained—in a now canonical line—that the Fourth Amendment "protects people, not places."[18] In addition, in a concurring opinion that created what is now known as the "*Katz* test," Justice Harlan explained that a Fourth Amendment "search" occurs when the government intrudes upon a "reasonable expectation of privacy."[19] This test consists of both a subjective and an objective prong and asks whether an individual exhibited an actual expectation of privacy, and if so, whether that expectation was one society recognizes as reasonable.

Katz was a watershed moment in Fourth Amendment law. Under its privacy-based approach, the Fourth Amendment's protections—which were once limited to an individual's private property—were extended to places including the interior of cars, luggage, public restrooms, hospital rooms, changing rooms, hotel rooms, and workplaces.[20] The meaning of its reference to "privacy," however, has been the subject of much confusion.[21]

[15] Id. at 456–57, 466.

[16] 389 U.S. 347 (1967).

[17] These technologies were beginning to lead to technical and arbitrary distinctions. For example, the Court held that a Fourth Amendment search had not occurred when a listening device was placed against a wall to monitor conversations in an adjacent office in *Goldman v. United States*, 316 U.S. 129, 135 (1942), but that a search had occurred when a "spike mike" penetrated through the defendants' wall in *Silverman v. United States*, 365 U.S. 505, 509–12 (1961).

[18] *Katz*, 389 U.S. at 347.

[19] Id. at 360 (Harlan, J., concurring).

[20] See Allyson W. Haynes, Virtual Blinds: Finding Online Privacy in Offline Precedents, 14 Vand. J. Ent. & Tech. L. 603, 621–22 nn.120–25 (2012) (citing cases).

[21] The test has been criticized as circular, vague, and ungrounded in the text of the Fourth Amendment. See, e.g., 1 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 2.1(d), at 393–95 (3d ed. 1996) (describing the test as tautological); Tracey Maclin, What Can Fourth Amendment Doctrine Learn from Vagueness Doctrine?, 3 U. Pa. J. Const. L. 398, 428–29 (2001) (asserting that the Court's expectations of privacy analysis

B. Privacy in the Fourth Amendment

In order to understand the concept of privacy embedded in the *Katz* test, one must appreciate the difference between descriptive and normative conceptions of privacy—a topic that has received insufficient attention in the literature. It is therefore worth taking a moment to clarify some of the core distinctions between and within these categories before turning to an analysis of the conception of privacy that is adopted in Fourth Amendment jurisprudence.

1. Normative vs. Descriptive Conceptions of Privacy

Normative conceptions of privacy, which dominate the privacy scholarship, define privacy in terms that incorporate into its meaning the idea that privacy is a good thing that deserves moral and legal protection. There are two general forms that this approach takes.

The first defines privacy in terms of the values, or human goods, that privacy fosters or protects. On this type of definition, saying that information about an activity or object is "private" means that it is involved in maintaining or fostering these goods or values. For example, the statement "my inner thoughts are private" might mean something like "my inner thoughts are integral to my autonomy." This is perhaps the most common approach to defining privacy and can be found in a wide range of scholarship. Some scholars focus on values that are individually-centered, such as dignity,[22] individuality,[23] and autonomy;[24] others focus on values that are interpersonal, such as friendship,[25] inti-

"rests on the *ad hoc* conclusions of the Justices"); Richard A. Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 Sup. Ct. Rev. 173, 188 (asserting that the Court's reasoning is circular, and its application of this test is inconsistent).

[22] See, e.g., Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev. 962, 971 (1964) (explaining that privacy protects an "individual's independence, dignity and integrity").

[23] See, e.g., Jeffrey H. Reiman, Privacy, Intimacy, and Personhood, 6 Phil. & Pub. Aff. 26, 44 (1976) ("The right to privacy . . . protects the individual's interest in becoming, being, and remaining a person."); Jed Rubenfeld, The Right of Privacy, 102 Harv. L. Rev. 737, 784 (1989) (explaining that privacy is "the fundamental freedom not to have one's life too totally determined by a progressively more normalizing state").

[24] See, e.g., Ruth Gavison, Privacy and the Limits of Law, 89 Yale L.J. 421, 423 (1980) (arguing that privacy is valuable in furthering liberty, autonomy, and freedom).

[25] See, e.g., James Rachels, Why Privacy Is Important, 4 Phil. & Pub. Aff. 323, 326 (1975) ("[T]here is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people.").

macy,[26] and love.[27] But the key point is that they all take privacy claims to be claims about the protection of certain human goods or values.

The second way in which privacy is defined as a normative concept is as a prescriptive feature of certain types of information. On this approach, saying that information about an activity or object is "private" means that it is a type of information that others should not try to discover. For example, as Stanley Benn argues, "private affairs" are not those that are actually "kept out of sight or from the knowledge of others," but rather those "that it would be inappropriate for others to try to find out about . . . without one's consent."[28] Two features of this general approach are worth highlighting. One is that only certain types of information can be properly classified as "private." For example, Tom Gerety argues that information only implicates privacy concerns if it is related to intimacy, identity, or autonomy.[29] Likewise, Richard Parker argues that a loss of secrecy does not always involve a loss of privacy, citing as an example a test that reveals that a given student did not study.[30] Another important feature of this general approach is that information can be private even if it is known to others.[31] For example, Dan Solove argues that there are activities that "we deem as private" that do not occur in secret: "The books we read, the products we buy, the people we associate with—these are often not viewed as secrets, but we nonetheless

[26] See, e.g., Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America 8 (2000) ("[I]ntimate relationships on which true knowledge of another person depends need space as well as time: sanctuaries from the gaze of the crowd . . . ."); Robert S. Gerstein, Intimacy and Privacy, 89 Ethics 76 (1978) ("[I]ntimate relationships simply could not exist if we did not continue to insist on privacy for them.").

[27] See, e.g., Charles Fried, Privacy, 77 Yale L.J. 475, 477, 483 (1968) (defining privacy as "control over knowledge about oneself" that is necessary to protect "fundamental relations" of "respect, love, friendship and trust").

[28] Stanley I. Benn, Privacy, Freedom, and Respect for Persons, *in* Privacy 1, 2 (J. Roland Pennock & John W. Chapman eds., 1971) (emphasis added).

[29] Tom Gerety, Redefining Privacy, 12 Harv. C.R.-C.L. L. Rev. 233, 281–95 (1977).

[30] Richard B. Parker, A Definition of Privacy, 27 Rutgers L. Rev. 275, 282 (1974). Daniel Solove makes a similar point, arguing that "there is a significant amount of information identifiable to us that we do not deem as private." Daniel J. Solove, Conceptualizing Privacy, 90 Calif. L. Rev. 1087, 1111–12 (2002). He suggests, for example, that the fact that a person is a well-known politician is identifiable to that person, but that this fact does not implicate privacy. Id. at 1112.

[31] For a discussion of scholars advancing this general view, see Solove, supra note 30, at 1108–09.

view them as private matters."[32] And along similar lines, Judith DeCew argues that "private matters" are not always secret, citing debts as an example.[33]

Descriptive accounts of privacy, by contrast, define it as a value-neutral condition or state of affairs. Unlike normative accounts, these accounts allow one to refer to states of increased and decreased privacy without taking a stance on the normative question of whether these states are good or bad. It is again helpful to distinguish between two general types of ways in which scholars have defined privacy in value-neutral terms.

The first defines privacy in physical terms as a state of isolation or seclusion. This idea is a component of the normative conception of privacy that Warren and Brandeis advance in The Right to Privacy, where they define privacy as the "right to be let alone,"[34] as well as the privacy tort of intrusion upon seclusion that their work inspired.[35] This notion is also a component of a number of "limited access to the self" conceptions of privacy,[36] including the purely descriptive account of Ruth Gavison, who writes: "Individuals lose privacy when others gain physical access to them. Physical access here means physical proximity—that *Y* is close enough to touch or observe *X* through normal use of his senses."[37]

The second type of descriptive account of privacy defines it in informational rather than physical terms. This category includes the widely advanced idea that privacy is a form of informational control. For example, Alan Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent

[32] Id. at 1109; see also id. at 1104 ("Certainly not all access to the self infringes upon privacy—only access to specific dimensions of the self or to particular *matters* and information." (emphasis added)).

[33] Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics, and the Rise of Technology 48 (1997).

[34] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 193 (1890).

[35] Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 553 (2006) ("One of the torts inspired by Warren and Brandeis's article is intrusion upon seclusion, which creates a cause of action when one intrudes 'upon the solitude or seclusion of another or his private affairs or concerns' if the intrusion is 'highly offensive to a reasonable person.'" (quoting Restatement (Second) of Torts § 652B)).

[36] See generally Solove, supra note 30, at 1102–05 (providing an overview of "limited access" conceptions of privacy).

[37] Gavison, supra note 24, at 433.

information about them is communicated to others."[38] Although this definition is often advanced in the context of normative theories that focus on the values served by the ability to control information about oneself,[39] the definition itself is value neutral.[40] The other main approach in this category defines privacy in terms of limitations on access to information about a person. This definition of privacy can stand alone, but is most often advanced as an element of a broader account that focuses on limited access to the self, of which information is one part. For example, Anita Allen defines privacy as "a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others."[41] The key point here is that unlike the more widely advanced definition that focuses on informational control, this approach focuses on knowledge: it is an "epistemic" conception of privacy.

2. The Supreme Court's Epistemic Conception of Privacy

Although privacy scholars have overwhelmingly defined privacy in normative terms, this is not the approach that the Supreme Court has taken in its Fourth Amendment jurisprudence. Rather, the conception of privacy embedded in the "reasonable expectation of privacy" test is the purely descriptive, epistemic conception identified above. Thus, the Fourth Amendment's protections are not defined or limited along either

[38] Alan F. Westin, Privacy and Freedom 7 (1970); see also Fried, supra note 27, at 482 ("Privacy is . . . the control we have over information about ourselves." (emphasis omitted)); Parker, supra note 30 at 281 ("[P]rivacy is control over when and by whom the various parts of us can be sensed by others." (emphasis omitted)).

[39] See, e.g., Solove, supra note 30, at 1109–15 (discussing these approaches).

[40] While this approach to defining privacy is common, there are two core problems with defining privacy in terms of informational control. The first is illustrated by a situation in which an individual controls the disclosure of a piece of information about himself. This person clearly loses privacy in the information that he discloses, even though he is in control of it, which means that control is not sufficient for privacy. The second problem is illustrated by the opposite situation, in which an individual is prohibited from sharing a piece of private information about himself. This person clearly has privacy in that piece of information, even though he lacks control over it, which means that control is not necessary for privacy. In short, these situations illustrate that control is neither necessary nor sufficient for a piece of information to remain private.

[41] Anita L. Allen, Uneasy Access: Privacy for Women in a Free Society 15 (1988). Allen argues that there are three ways in which a person can be inaccessible: "physically, dispositionally, and informationally." Id. at 16; see also Gavison, supra note 24, at 428 (suggesting that "an individual enjoys *perfect* privacy when he is completely inaccessible to others").

of the normative dimensions that have been the focus of privacy scholars.

a. Value-Based Conceptions

With respect to the value-based conceptions of privacy that have been developed by privacy scholars, two points are worth highlighting: The Fourth Amendment's protections do not turn on the values served by protecting the secrecy of a piece of information in a given case, nor do they depend on the social value of the means by which this secrecy is maintained.

On the first point, a person can have a constitutionally-protected "reasonable expectation of privacy" that has nothing to do with the personal or interpersonal values that have been the focus of privacy scholars. This feature of Fourth Amendment jurisprudence can be seen clearly in *Arizona v. Hicks*.[42] In this case, police officers had legally entered an apartment to investigate a shooting, but upon entering, noticed expensive-looking stereo equipment and turned it over to copy down the serial number.[43] The Supreme Court found that looking at the underside of the stereo equipment was a separate search that needed to be justified independently of the original search[44]—a result that does not make sense under a values-based conception of privacy, such as a dignitary conception. As Bill Stuntz has argued, under a dignitary conception of privacy, "what happened in *Hicks* would not be worth worrying about: turning over the stereo caused no real dignitary harm. In dignitary terms the only issue would be the legality of the search of the apartment *in general*."[45] On the purely informational approach of the Court, however, "each marginal search, each additional place where the officer casts his eye, represents a separate issue."[46]

On the second point, the Fourth Amendment's protection does not turn on the value, or importance, of preventing government intrusion into a given area. Although *Katz* highlighted "the vital role that the public telephone has come to play in private communication,"[47] the Supreme

[42] 480 U.S. 321 (1987).
[43] Id. at 323.
[44] Id. at 324–25.
[45] William J. Stuntz, Privacy's Problem and the Law of Criminal Procedure, 93 Mich. L. Rev. 1016, 1023 (1995).
[46] Id.
[47] Katz v. United States, 389 U.S. 347, 352 (1967).

Court has not subsequently taken such considerations into account when deciding whether to extend the Fourth Amendment's protections to the interior of cars, luggage, public restrooms, hospital rooms, changing rooms, hotel rooms, and workplaces.[48] Under the Court's approach, the inside of a paper bag receives the same protection as the inside of a home.[49] One might argue, however, that an echo of this idea from *Katz* can be seen in the recent case of *Riley v. California*.[50] As the Court framed it, this was a case about "how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[51] Although this case concerned exceptions for search warrants—rather than the nature of searches and the meaning of privacy under the *Katz* test—the fact that the Court held that a warrant is generally required to search cell phones seized incident to an arrest (thereby removing them from the scope of a well-established doctrine) could be seen as a sign that the Court is willing to weigh the importance of a type of personal effect in its Fourth Amendment analysis. Yet, as in *Katz*, the importance of the cell phone ultimately played little role in the Court's analysis in *Riley*. Its decision to treat cell phones differently from other types of personal effects was based primarily on the quantity of personal data at issue (for example, the number of photos in a phone versus a wallet), rather than a value-based conception of privacy.[52]

Thus, there is a disconnect between the value-laden conceptions of privacy that have been the focus of privacy scholars, and the purely de-

[48] See Haynes, supra note 20 (citing cases).

[49] United States v. Ross, 456 U.S. 798, 822–23 (1982) (holding that it would be improper to draw "a constitutional distinction between 'worthy' and 'unworthy' containers" and that "the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view").

[50] 134 S. Ct. 2473 (2014).

[51] Id. at 2484.

[52] Id. at 2489–90 (discussing considerations related to the amount of data that can be stored in a cell phone, compared to nondigital forms of storage); id. at 2490 (discussing the number of people who carry cell phones, compared to the number of people who carry diaries and other nondigital forms of data); id. at 2491 (discussing the data about a person that can be revealed by searching a cell phone, compared to searching a house). While the Court also noted that certain types of data stored on a phone are "qualitatively different" than physical records, the examples that it provides—data about one's addictions, religion, medical conditions, finances, hobbies, sexual orientation, etc.—could equally be found in a diary. Id. at 2490. Further, as I argue below, it is well established that the type of information at issue in a search is irrelevant to the *Katz* test.

scriptive, epistemic conception of privacy that is embodied in the Fourth Amendment case law. This is not to say that the case law does not indirectly protect such values, as it is possible that this approach produces positive externalities—for example, by creating general zones of protection. In this sense, the protection of information that is unrelated to these values could be seen as an example of over-breadth, which might be more effective than a case-specific approach, and perhaps even necessary. But this is beside the point here. What matters here is that the "reasonable expectation of privacy" test does not incorporate a value-based conception of privacy.

b. Types of Information

The Supreme Court's Fourth Amendment jurisprudence also rejects the common notion that "privacy" is a prescriptive characteristic that applies only to certain types of information. Under the Supreme Court's approach, it is neither necessary nor sufficient that a government intrusion implicate a given type of information to violate the Fourth Amendment.[53]

The fact that the Fourth Amendment's protections do not apply only to certain types of information—that this is not a necessary condition—can be seen clearly in *Kyllo v. United States*,[54] where the Court explicitly rejected the government's argument that the Fourth Amendment's protections were in any way connected to the nature of the information at issue. The Court held that "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the *quality or quantity* of information obtained."[55] Although the Court elsewhere stated that "[i]n

[53] While a normative analysis of the desirability of the Court's approach is outside the scope of my project, it is worth noting that it does have some benefits. For example, courts do not need to try to classify some *types* of information as inherently private and others as inherently public, which is a more difficult task than it might seem. As Marc Blitz explains:

> While some public activities, such as going to a doctor, may seem more personal than others, such as walking on a street with a friend, the importance of privacy in each situation will depend heavily on contextual details—What kind of a doctor's visit is it? Who is the friend one is walking with?—and will differ considerably from person to person.

Marc Jonathan Blitz, Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity, 82 Tex. L. Rev. 1349, 1412 (2004).

[54] 533 U.S. 27 (2001).

[55] Id. at 37 (emphasis added). In addition, the Court held that this approach would be impracticable in application, as it would not provide a workable accommodation between law

the home . . . *all* details are intimate details" (which some have read as supporting a "private facts" model of the Fourth Amendment), the Court clarified that the concept "intimate" did not refer to specific *types* of information, but rather to any information that was "otherwise imperceptible to police or fellow citizens."[56] Likewise, in *Arizona vs. Hicks*,[57] the Court emphasized the irrelevance of the type of information at issue. In holding that a police officer had violated the Fourth Amendment when he picked up a piece of stereo equipment and looked at the bottom for serial numbers, the Court explained: "It matters not that the search uncovered nothing of any great personal value to respondent . . . . A search is a search, even if it happens to disclose nothing but the bottom of a turntable."[58]

Conversely, the fact that the Fourth Amendment's protections do not apply merely because of the type of information at issue—that this is not a sufficient condition—is illustrated by *California v. Greenwood*,[59] where the Court held that rifling through a person's trash did not violate a reasonable expectation of privacy, despite the intimate information that could be revealed. As noted by Justice Brennan in dissent:

> A search of trash, like a search of the bedroom, can relate intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target's financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests.[60]

But the Court rejected the relevance of such considerations.

It is worth noting, however, that there is some confusion in the privacy literature on this aspect of the Court's Fourth Amendment jurisprudence, and that some scholars have argued that the Supreme Court sometimes applies a "private facts model" of the Fourth Amendment.

enforcement needs and Fourth Amendment interests, and would require the development of "jurisprudence specifying which home activities are 'intimate' and which are not." Id. at 38–39.

[56] Id. at 37, 38 n.5 (explaining that its prior references to "intimate details" did not actually focus "upon intimacy but upon otherwise-imperceptibility, which is precisely the principle we vindicate today").

[57] 480 U.S. 321 (1987).

[58] Id. at 325.

[59] 486 U.S. 35 (1988).

[60] Id. at 50 (Brennan, J., dissenting).

According to Orin Kerr, for example, the Court will at times consider "whether the government's conduct reveals particularly private and personal information deserving of protection"; and this factor can be decisive in both directions: "If the government obtains information that is particularly private, then the acquisition of that information is a search; if the information collected is not private or does not otherwise merit protection, then no search has occurred."[61] However, a close reading of the case law does not support this normative "private facts" model of Fourth Amendment protection.

Take, for example, *United State v. Karo*, which is the only case Kerr cites to support his claim that a private facts model has been used to justify a finding of a Fourth Amendment violation.[62] In this case, the Court held that the government had violated the Fourth Amendment in placing a tracking device inside a can of chemicals that was subsequently brought inside a private home. The Court explained that the government conduct was a search because it revealed "a critical fact."[63] Here, it might seem that the "critical fact" was critical because it concerned "intimate matters" or some other *type* of so-called "private information." However, read in context, it is clear that the fact was "critical" merely because it was "a fact that could not have been visually verified" and "could not have otherwise [been] obtained without a warrant."[64] It was "private" only in the sense of being inaccessible to the public—just as the facts in *Kyllo* were "intimate" only in the sense of being "otherwise imperceptible to police or fellow citizens."[65]

Likewise, in the limited cases in which the Court has rejected Fourth Amendment protection based on the content of the information at issue,

[61] Orin S. Kerr, Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 506, 512–13 (2007).

[62] 468 U.S. 705 (1984).

[63] Id. at 715.

[64] Id.

[65] *Kyllo*, 533 U.S. at 38 n.5 (explaining that its prior references to "intimate details" did not actually focus "upon intimacy but upon otherwise-imperceptibility, which is precisely the principle we vindicate today"). In general, when the Court considers the content of information in a Fourth Amendment analysis, it is only to determine whether that information was exposed. See, e.g., United States v. Miller, 425 U.S. 435, 442 (1976) ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents . . . . All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

the determinative issue has not been whether the alleged search might have yielded information pertaining to "private matters," but rather whether it might have yielded *any* information that was not evidence of a crime. For example, the Court has held that testing a powder to see if it is cocaine[66] or allowing a dog to sniff a bag for drugs[67] are not searches on the grounds that they can reveal nothing other than evidence of a crime. These opinions do not adopt or rely on any conception of what makes a fact "private." Rather, the issue is whether the search could have revealed any information other than evidence of a crime, which the Court has held is unprotected by the Fourth Amendment.

Thus, while there is language in some Supreme Court opinions that might seem to suggest that the type of information at issue can be relevant to the Fourth Amendment analysis, closer analysis reveals that it is neither necessary nor sufficient that a government intrusion implicate a given type of information to violate the Fourth Amendment. When the Court refers to "intimate" information in Fourth Amendment cases, it means nothing more than information that is "otherwise imperceptible to police or fellow citizens."[68] Or as Bill Stuntz put it:

> When courts decide whether a given police tactic infringed a "reasonable expectation of privacy" and hence whether the tactic is a "search" subject to Fourth Amendment regulation, they ask whether the police saw or heard something that any member of the public might have seen or heard in a similar manner. The question, in other words, is whether what the police did was likely to capture something secret.[69]

C. The Limits of the Privacy Framework

Recognizing that the Supreme Court has adopted an epistemic conception of privacy in its Fourth Amendment jurisprudence helps explain two doctrines that limit the law's protections of personal information based on the accessibility of that information. While it is often said that *Katz* marked a categorical expansion of the scope of the Fourth Amendment's protections, the reality is not this simple. The reason is

[66] United States v. Jacobsen, 466 U.S. 109, 122–125 (1984).
[67] Illinois v. Caballes, 543 U.S. 405, 408–410 (2005).
[68] *Kyllo*, 533 U.S. at 38 n.5.
[69] Stuntz, supra note 45, at 1021; see also id. at 1017 ("Privacy, at least as the word is used in criminal procedure, protects the interest in keeping information out of the government's hands.").

that in concluding that it is privacy, not property, that matters, the Court explained: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[70] In context, this remark emphasized the latter half of the statement—that people can maintain their privacy despite being in a public place. However, subsequent cases reiterating this statement have shifted focus to the first half. In addition, while *Katz* explained that someone's exposed activities "are not 'protected' because no intention to keep them to himself has been exhibited"[71] (implying that clear intent to the contrary would be relevant), the Court has since abandoned this limiting rationale. This can be seen in two doctrines that exempt certain types of information from the scope of the Fourth Amendment's protections.

1. The Public Exposure and Third Party Doctrines

The first limitation is known as the "plain view" or "public exposure" doctrine, under which "the police are not subject to any Fourth Amendment constraint when they see something from a vantage point they are entitled to take (sometimes because any member of the public is entitled to the same vantage point)."[72] The logic of this limitation is the "centerpiece" of search law according to Bill Stuntz, who has highlighted that it "basically defines what is a 'search,' and hence defines what police conduct the Fourth Amendment regulates and what conduct it leaves alone. With respect to things that are searches, the plain view concept determines what must be separately justified."[73]

A series of cases involving aerial surveillance of private property are helpful in illustrating the "public exposure" aspect of this doctrine. In *California v. Ciraolo*,[74] for example, the Supreme Court held that a "naked-eye" aerial observation of a fenced-in curtilage of a home did not constitute a search under the Fourth Amendment on the grounds that the plane was flying at a height where "private and commercial flight . . . is routine," such that "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers ob-

[70] *Katz*, 389 U.S. at 351–52.
[71] Id. at 361 (Harlan, J., concurring).
[72] Stuntz, supra note 45, at 1022.
[73] Id.
[74] 476 U.S. 207 (1986).

served."[75] And expanding on this logic in *Dow Chemical Co. v. United States*, the Court held that the police could even assist their fly-over surveillance with a powerful aerial mapping camera capable of identifying objects as small as one-half inch in diameter, explaining: "The mere fact that human vision is enhanced somewhat . . . does not give rise to constitutional problems."[76] Nor are such problems created by "the mere fact that an individual has taken measures to restrict some views of his activities."[77] In *Florida v. Riley*, for instance, the Court reached the same conclusion when the police used a helicopter flying at four hundred feet above the ground to observe marijuana plants growing in a greenhouse by looking through missing panels in the greenhouse roof.[78]

The Court has also followed this logic in cases of surveillance using tracking devices. For example, in *United States v. Knotts*, the police placed an electronic tracking beeper in a can of chloroform, which the defendant then purchased and placed in his car, which the police then tracked using the beeper.[79] The Court held that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," as the surveillance "amounted principally to the following of an automobile on public streets and highways."[80] Addressing the difference in technology used, the Court held that the fact that the movements were detected with a beeper rather than visual surveillance "does not alter the situation."[81]

The second and conceptually related doctrine is known as the "third party doctrine," under which the Court has held that there is no reasonable expectation of privacy in information that is conveyed or known by third parties, even if the information was conveyed in confidence. The foundational case for this doctrine is *United States v. Miller*, in which the Court held that the Fourth Amendment does not apply to bank records.[82] In this case, federal investigators subpoenaed the defendant's

[75] Id. at 213–15.
[76] 476 U.S. 227, 238 (1986).
[77] *Ciraolo*, 476 U.S. at 213.
[78] 488 U.S. 445, 451 (1989).
[79] 460 U.S. 276 (1983).
[80] Id. at 281.
[81] Id. at 282. With rare exceptions, courts have extended this logic to find that camera surveillance of public places also does not constitute a search. See Christopher Slobogin, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, 72 Miss. L.J. 213, 236–37 (2002) (citing cases).
[82] 425 U.S. 435 (1976).

bank records without a warrant, and the records revealed that he had written checks to buy equipment used to distill black-market whiskey. When the defendant claimed that these subpoenas violated his Fourth Amendment rights, the Court explained that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[83] For this reason, the Court explained, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[84]

Expanding on this logic in *Smith v. Maryland*, the Court held that the Fourth Amendment likewise does not protect one's phone records from a warrantless search.[85] In this case, the officers had used a pen register installed at a phone company's office to record the numbers that the suspect had dialed. The Court reasoned that the suspect had voluntarily exposed the digits to the switchboard, which it saw as "merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[86] The Court held that because people "know that they must convey numerical information to the phone company," they cannot "harbor any general expectation that the numbers they dial will remain secret."[87]

In sum, the Supreme Court has held that the Fourth Amendment does not protect information that has been exposed to others, even if it would be highly unlikely or nearly impossible in practice for the public to obtain this information. And while the concurring opinions of Justices Alito and Sotomayor in *United States v. Jones* revealed that five members of the Court question the applicability of these doctrines to some cases of long-term surveillance, neither opinion articulated a rule or standard that would identify these cases—a topic to which I will return below.[88]

---

[83] Id. at 443.

[84] Id.

[85] 442 U.S. 735 (1979).

[86] Id. at 744.

[87] Id. at 743.

[88] In *United States v. Jones*, Justices Alito, Ginsburg, Breyer, and Kagan would have held that the twenty-eight-day-long GPS tracking of the defendant's car violated his reasonable expectations of privacy. 132 S. Ct. 945, 958 (2012) (Alito, J., concurring). And while Justice Sotomayor expressed sympathy with this view in a concurrence, she ultimately joined the other members of the Court in the narrower holding that placing the GPS on the car violated the Fourth Amendment on the grounds that it involved trespass onto the defendant's private property. Id. at 954 (Sotomayor, J., concurring). In addition, Justice Sotomayor suggested

2. The Critical Scholarship

In the privacy scholarship, there is widespread agreement that the failure of the Fourth Amendment jurisprudence to protect information that is known to third parties or potentially accessible to the public is based on an overly simplistic and binary conception of privacy. This critique has been articulated in conceptual, empirical, and sociological terms, but underlying these different articulations is the same core claim that courts have failed to recognize that privacy can exist in degrees.[89] Three frequently cited critiques are illustrative of this general position.

The first, by Dan Solove, frames the judicial error in conceptual terms.[90] Solove argues that courts are operating under a misguided "secrecy paradigm" in which privacy is conceptualized as "complete secrecy" and "a privacy violation occurs when concealed data is revealed to others."[91] The core problem with this understanding of privacy, Solove argues, is that it misconceives privacy as a binary matter, failing to recognize the multitude of ways in which privacy can exist in degrees. For example, it fails to recognize that we can "keep things private from some people but not others,"[92] and that "there is a considerable loss of

that it "may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Id. at 957. Some circuit courts have in fact rejected the third party doctrine in electronic information cases. See, e.g., United States v. Warshak, 631 F.3d 266, 286–87 (6th Cir. 2010) ("[T]he mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."); United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007) ("[T]he mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer.").

[89] See, e.g., LaFave, supra note 21, § 2.1(d), at 394 ("[T]oo often the Court has failed to appreciate that 'privacy is not a discrete commodity, possessed absolutely or not at all,' and that there is a dramatic difference, in privacy terms, between revealing bits and pieces of information sporadically to a small and often select group for a limited purpose and a focused police examination of the totality of that information regarding a particular individual." (citation omitted)).

[90] This is one of the most frequently cited critiques. See, e.g., Woodrow Hartzog & Frederic Stutzman, The Case for Online Obscurity, 101 Calif. L. Rev. 1, 17–20 (2013) (drawing on Solove's "secrecy paradigm" critique); Katrina Fischer Kuh, Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms, 65 Vand. L. Rev. 1565, 1604–07 (2012) (same); Andrew J. DeFilippis, Note, Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence, 115 Yale L.J. 1086, 1091–94 (2006) (same).

[91] Solove, supra note 35, at 497.

[92] Solove, supra note 30, at 1108; see also Mary I. Coombs, Shared Privacy and the Fourth Amendment, or the Rights of Relationships, 75 Calif. L. Rev. 1593, 1593 (1987) ("[C]urrent

privacy by plucking inaccessible facts buried in some obscure document and broadcasting them to the world on the evening news."[93] Furthermore, Solove argues, this conception of privacy is self-defeating; for insofar as we live in a world in which it is virtually impossible to avoid leaving a trail of personal information wherever we go, the secrecy paradigm's conception of privacy ultimately commits us to a world without privacy.[94] Solove argues that courts should therefore abandon this overly restrictive conception of privacy and focus instead on the wide variety of harms that people identify and experience as privacy violations.[95]

A second critique, by Lior Strahilevitz, frames the judicial error in empirical terms.[96] Drawing on a body of "social networks" literature that has identified many of the factors that determine whether a piece of personal information will be widely distributed after it is first disclosed, Strahilevitz argues that courts deciding privacy cases have missed many of the relevant considerations:

> In order to determine whether a particular fact known by some people will become widely publicized, one needs to know much more than how many people are currently aware of the fact. Rather, one needs to know where, within a social network, this information exists; what types of people have access to it; what the incentives are for subsequent dissemination; whether the information must be aggregated with other forms of information in order to become pertinent; and what

Fourth Amendment jurisprudence is impoverished and distorted by neglecting the ways in which privacy embodies chosen sharing.").

[93] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 44 (2004). With respect to the Fourth Amendment, Solove notes: "*Katz* purported to usher in a wide scope of Fourth Amendment coverage based on a broad understanding of privacy. Instead of expanding its understanding of privacy, however, the Court merely shifted its view, conceiving of privacy as a form of total secrecy." Daniel J. Solove, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference, 74 Fordham L. Rev. 747, 751 (2005).

[94] Daniel J. Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 Minn. L. Rev. 1137, 1177 (2002).

[95] Solove, supra note 35, at 563. For example, with respect to surveillance, he argues that courts should not focus on whether the surveillance occurs in public or in private, but rather on the aggregation of data, which can create harms even when all of the data are already available in the public domain. Id. Or with respect to disclosure, he argues that the focus should not be on whether the information is known to third parties, but rather on whether it is being spread beyond expected boundaries. Id.

[96] See, e.g., Lior Jacob Strahilevitz, A Social Networks Theory of Privacy, 72 U. Chi. L. Rev. 919, 921 (2005) (arguing that we should treat the privacy "question as an empirical one").

> kinds of social norms facilitate or constrain subsequent dissemination of the information.[97]

These factors can explain why information that is "known by one hundred people might never be disseminated further, but the widespread dissemination of other information known to only two people might be inevitable."[98] Thus, by identifying the ways in which these types of factors will operate, Strahilevitz argues, the literature on social networks "can help provide courts with a coherent and consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that he has shared with one or more persons."[99] The existence of a reasonable expectation of privacy, on this account, is a purely empirical one: It turns on the probability that a given piece of information would have become widely distributed absent some defendant's actions.

The third critique, by Helen Nissenbaum, frames the problem in sociological terms. Nissenbaum argues that the courts have mistakenly divided the world into a "private/public dichotomy" in which norms governing the disclosure of personal information only apply to information in the private sphere.[100] Against this view, Nissenbaum argues that there are no spheres of life that are not governed by information-sharing norms, and furthermore, that these norms are contextual in ways that the place-based public/private dichotomy fails to recognize: "Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation."[101] Focusing on these contextual factors, Nissenbaum proposes a theory of privacy "as contextual integrity" in which privacy violations occur when the disclosure of a piece of personal information disrespects the context in which the information was originally shared. On this account, "a right to privacy is neither a right to se-

[97] Id. at 922.
[98] Id.
[99] Id. at 919.
[100] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 113–25 (2010) [hereinafter Nissenbaum, Privacy in Context]; Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119, 136 (2004) [hereinafter Nissenbaum, Privacy as Contextual Integrity].
[101] Nissenbaum, Privacy as Contextual Integrity, supra note 100, at 137.

crecy nor a right to control but a right to *appropriate* flow of personal information."[102]

In sum, the privacy literature contains a variety of critiques of the third party and public exposure doctrines, but each provides a similar diagnosis. They all suggest that the core problem is that courts have failed to recognize that privacy is not a binary condition, but rather something that exists in degrees, and that various types of barriers can prevent a fact about an identified person from travelling from a limited private audience to the public at large. While I agree that this critique is correct as far as it goes, I will argue that it only identifies part of the problem.

II. PRIVACY VS. ANONYMITY

The problem with the public exposure and third party doctrines is not only that they fail to recognize that a piece of personal information can be protected in varying degrees, as privacy scholars have long argued. In addition, and more fundamentally, they conflate two distinct forms that this protection can take: privacy and anonymity. In order to explain the significant implications of this mistake, Section A will differentiate the generally conflated concepts of anonymity and privacy. Section B will then clarify the nature of anonymity, which has received insufficient attention in the academic literature and is often misunderstood. Finally, Section C will demonstrate that this analysis reveals the reasons why and ways in which the Fourth Amendment should be interpreted to protect not only reasonable expectations of privacy, but also "reasonable expectations of anonymity."

A. Differentiating Privacy and Anonymity

The fundamental problem with the Fourth Amendment jurisprudence that has not yet been identified in the critical scholarship is that courts have recognized only one of two ways in which a piece of information about someone can remain unknown to others. This state of affairs is, as discussed above, one that determines whether the Fourth Amendment's protections apply. When courts refer to informational "privacy," what they mean is that a piece of personal information is unknown. But courts have failed to recognize one of two ways in which this condition might present itself.

[102] Nissenbaum, Privacy in Context, supra note 100, at 127.

To see what courts have missed, it is helpful to start by thinking about a piece of personal information as consisting of two core elements: a subject (which identifies the person at issue) and a predicate (which informs us of some fact about that person). For example, the fact that Abraham Lincoln delivered the Gettysburg Address consists of a subject ("Abraham Lincoln") and a predicate ("delivered the Gettysburg Address"). The same is true of all other pieces of personal information, which can be disaggregated into these components and cross-connected, as this table illustrates:

Subject	**Predicate**
• Abraham Lincoln • The 16th United States president • The 2nd child of Thomas Lincoln	• delivered the Gettysburg address • was the first president to be assassinated • received Patent No. 6469 for a device to lift boats over shoals

We could say "the second child of Thomas Lincoln . . . delivered the Gettysburg Address," or "the 16th United States president . . . received Patent No. 6469 for a device to lift boats over shoals," etc. Any combination of subject and predicate will be a true statement about the same person.[103]

Thinking in these terms is valuable in several ways. Perhaps the most important is that it helps clarify the difference between anonymity and privacy, as I will demonstrate next. To see the difference, however, it is helpful to first conceptualize "knowing something about someone" as knowing an element from both columns. This is a simple point, but it is important as it highlights that there are two ways of preventing others from learning or accessing a given "personal fact." This can be accomplished by either hiding what makes it "personal" (the subject) or hiding the "fact" (the predicate).[104]

[103] It is worth highlighting that the issue of whether something belongs in the subject or predicate column is not fixed, but rather depends on context and the issue of what is unknown. For example, "the 16th U.S. president" is in the subject column above, where it refers to a person about whom some facts are unknown. But one could also write "was the 16th U.S. president" in the predicate column, where it would be a fact about someone whose identity could be unknown. Thus, it is not the type of information that determines whether it is a subject or predicate, but rather its place or function in a given piece of knowledge—which is an issue that I will return to in more detail below.

[104] There is also a third way, in which both of these components are unknown. This type of secrecy can be termed "deep secrecy," and plays an important role in government secrets.

Applied to Fourth Amendment jurisprudence, this distinction helps us see that courts have granted legal recognition to the second of these ways of hiding a piece of personal information (that is, hiding the fact), but not the first (that is, hiding what makes it personal). For example, if someone reasonably expects that a fact he conveys in a public phone booth will remain unknown to the public, courts have held that the police cannot engage in an activity, such as wiretapping, that would uncover and connect these statements to him. But if this person reasonably expects that his identity as a speaker of statements made in public will remain unknown, courts have held that the police can engage in an activity that will connect his identity to these statements, such as surveillance.

Courts have not, however, explicitly addressed why only the first mode of hiding personal information is relevant, nor have scholars criticized them for failing to do so. This lacuna in the jurisprudence and the academic literature can be explained as the result of a conceptual confusion, as the overlooked difference between these two ways of hiding information is the difference between the concepts of "privacy" and "anonymity," which have also been mistakenly conflated by courts and scholars.[105] This conflation of anonymity and privacy derives from the fact that both concepts have traditionally been defined solely in normative terms, which highlights the similar goals that they can serve. When the concepts are instead understood in descriptive terms, a fundamental distinction between them becomes clear.

The key difference between anonymity and privacy is that although both describe a state of affairs in which a piece of personal information is unknown to others, they describe opposite sides of this state of affairs.

See David E. Pozen, Deep Secrecy, 62 Stan. L. Rev. 257 (2010). But I am only interested in the two less complete forms of secrecy that are relevant to privacy law.

[105] It is often suggested that anonymity is one of several types of privacy. See, e.g., Alan F. Westin, Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I–The Current Impact of Surveillance on Privacy, 66 Colum. L. Rev. 1003, 1020 (1966) ("Privacy in the sense of being 'let alone' actually encompasses four different psychological and physical relations between an individual and those around him. These are the states of solitude, intimacy, anonymity, and reserve."); see also Gavison, supra note 24, at 428 (defining privacy as having three elements: secrecy, anonymity, and solitude); Slobogin, supra note 81, at 238–39 (building on Westin's suggestion that anonymity is a state of privacy). One can also find suggestions that anonymity is the perfect realization of privacy. See, e.g., Shawn C. Helms, Translating Privacy Values with Technology, 7 B.U. J. Sci. & Tech. L. 288, 301 (2001) ("Anonymity is not a subset of privacy; rather, it can be thought of as the perfect realization, or product of, privacy.").

To see this point, it is helpful to return to the "subject" and "predicate" columns above. Framed in these terms, privacy and anonymity can be defined as follows: When we know the subject of a sentence, but not a relevant predicate, we confront the condition of privacy; whereas when we know the predicate of a sentence, but not a relevant subject, we confront the condition of anonymity. For example, if we want to learn more about Abraham Lincoln, but cannot access any of the facts in the predicate column, the privacy of Lincoln is protected. Conversely, when we want to learn more about the recipient of Patent No. 6469, but cannot access any of the identifiers in the subject column, the anonymity of the patent is protected. In this sense, privacy and anonymity are flip sides of each other: They are distinct, but connected, describing opposite sides of a given state of affairs.[106]

Further, the reason that anonymity and privacy are flip sides of each other is that they are causally linked. Both describe a situation in which a piece of personal information is unknown to others because it has been split apart into these constituent elements. Anonymity and privacy exist on opposite sides of the "wall" that is created by splitting a person's identity from information about that person. If, post-split, we know the person's identity but not the information, we describe the condition as "privacy"; whereas if we know the information but not the person's identity, we describe the condition as "anonymity."

An example helps illustrate this point. Imagine that a person's medical file contains a piece of paper with the results from his blood test, but his doctor removes the paper and places it in a blank file (or in other words, he splits apart this piece of personal information). If we subsequently obtained access to this person's medical file, without the test results, we would describe the situation using the concept of privacy: We would say "the privacy of the person is protected," or "the associated information is private," etc. If, on the other hand, we obtained access to the test results, without the medical file, we would describe the situation using the concept of anonymity: We would say "the anonymity of the test results is protected," or "the associated person is anonymous," etc. Thus, anonymity and privacy refer to conditions that are created by the

[106] Note that the issue of whether we are confronted with privacy or anonymity depends on context. A central feature of this way of understanding anonymity and privacy—as incomplete knowledge of a given piece of personal information—is that a subject can become a predicate, and vice versa, depending on context.

same event: splitting a person's identity and a piece of information about that person.

Recognizing this causal connection between anonymity and privacy is especially important because it explains a source of some confusion in the literature: it explains why anonymity seems to protect privacy. It is not because anonymity is a type of privacy or because they are overlapping traits, as some scholars have suggested. Rather, it is because the existence of one entails the existence of the other. They are different sides of—or ways of looking at—the same thing. Where something is private, something is anonymous, and vice versa.

For example, in the above hypothetical, if we gain access to the test results but cannot identify them, the test results will be *anonymous*, and as a result *the privacy of the patient* with respect to the results will be protected. And conversely, if we gain access to the medical file but cannot find the test results, the patient's *privacy* will be protected, and as a result *the anonymity of the results* will be protected. The latter situation (in which anonymity is used to protect privacy) might appear to be less relevant, as it might appear that there are few situations in which our law is concerned about anonymity as an end, rather than a means of protecting privacy. But as I explore in other work, recognizing the difference between anonymity and privacy reveals countless areas of law that focus on anonymity rather than privacy.[107] The key point here, however, is just that where something is anonymous, something is private, and vice versa. Thus, my differentiation of the concepts does not reject, but rather explains, the idea that anonymity protects privacy.

In addition to explaining how privacy and anonymity can be used to protect each other, this account clarifies why they can be necessary to protecting each other.[108] The extent to which this is the case depends on the context and specificity of any disclosures. For instance, while some breaches of privacy (such as disclosing that a blood donor donated to a blood bank that contains only one sample) will eliminate the anonymity of the blood in the bank, others (such as disclosing that he donated to a bank with 100 samples) will only begin to chip away at the blood's anonymity. Likewise, while some breaches of anonymity (such as disclosing the name associated with a donated sample) will eliminate the priva-

[107] See Skopek, supra note 9, at 1759–69.

[108] They are not sufficient because other forms of disclosure can eliminate either anonymity or privacy.

cy of the donor's act of donation, others (such as disclosing identifiers associated with a donated sample) will only partly implicate his privacy.

Finally, one last important feature of the concepts revealed by my account is that both anonymity and privacy involve the public visibility of something. When we confront privacy, the person's identity is public, whereas when we confront anonymity, the disassociated things are public. Under neither are both the identity and things hidden; if they were, this would not be privacy or anonymity, but rather deep secrecy—or, an "unknown unknown."[109] Anonymity and privacy, by contrast, refer to publicly known unknowns. Recognizing this is important, as it clarifies a topic of some confusion: namely, why performing an action in public does not necessarily implicate the privacy of the actor, and why making the identity of an actor public does not necessarily implicate the anonymity of the action. The reason is that as long as the action's anonymity is preserved in the former case, and the actor's privacy is maintained in the latter, the foundational disaggregation of identity from attribute that constitutes both privacy and anonymity can be maintained.

In sum, when "personal information" is understood as an aggregation of two core components—a subject and a predicate—it becomes clear that there are two relevant ways in which it can be inaccessible to others. Under the first, we know the person's identity, but not the information. This type of secrecy is what we generally call privacy. Under the second, we know the information, but not the personal identity. This is what we generally call anonymity. This is, at least, how I understand the ordinary uses of these terms. Whether one agrees with this characterization of our ordinary language is not, however, crucial for my argument. For my point is merely to identify a previously unrecognized distinction between two ways of protecting the secrecy of one's personal information—a distinction that is relevant for sources of law that aim to protect this secrecy, including the Fourth Amendment.

B. The Nature of Anonymity

Before exploring the relevance of the above analysis for the Supreme Court's Fourth Amendment jurisprudence, it is worth clarifying in a bit more detail what it means for something to be anonymous. Because anonymity has generally been conceived of as a mere aspect or tool of pri-

[109] Pozen, supra note 104, at 259.

vacy,[110] it has received insufficient academic attention.[111] The following analysis will demonstrate that what it means to be "anonymous" is far more complex than it might at first seem.

Anonymity, like privacy, is often defined in terms of a type of information: it is suggested that to be "anonymous" is to be "nameless."[112] This definition is problematic in two ways that help clarify the true nature of anonymity. The first problem is that namelessness is not actually a sufficient condition for anonymity. A simple example illustrates this point. Imagine a situation in which I do not know my neighbor's name, but know every piece of art that he has produced. If I then see one of these pieces of art in a museum, it will not be anonymous to me because I will know that my neighbor produced it, regardless of whether it is labeled with his name. So while withholding a name is often an effective way of rendering something anonymous, withholding other information may be necessary (though in some cases, such as this artwork example, it may be impossible to do so without withholding all of the information about the object at issue). The second problem with the definition is that namelessness is also not a necessary condition for anonymity. Something can be named, but still anonymous. Take, for example, a book for which the author is listed as "John Smith." If there are thousands of people named "John Smith," the book will be effectively anonymous absent further information. Thus, in short, while withholding a name is often an effective way of rendering something anonymous, it is not always necessary, nor is it always sufficient: withholding other information may be necessary. So defining anonymity as namelessness is both under- and over-inclusive.

Furthermore, the same lessons apply to the relationship between names and identification. The above example of artwork shows that identification does not always require that the thing be named, and the example of the book shows that identification can require knowledge of more than the associated person's name. In the case of the book, for instance, we may need to link the name of the book's author with other

[110] See supra note 105 and accompanying text.

[111] The recent literature on the concept of privacy as obscurity perhaps comes closest to offering a rich discussion of some aspects of anonymity. See, e.g., Hartzog & Stutzman, supra note 90, at 32–40 (developing a nuanced definition of online obscurity).

[112] This definition can be found in the dictionary, see Webster's Third New International Dictionary 89 (1986), as well as the legal literature. See, e.g., Slobogin, supra note 81, at 238 ("The right to public anonymity provides assurance that, when in public, one will remain nameless . . . . ").

facts about the book (for example, the year and place of publication) to identify the author. Likewise, if I have two friends with the name "John Smith," I will need to combine this name with an additional fact or facts to identify the friend to whom I am referring (for example, "John Smith with red hair"). In short, while names are often effective means of identification, they are not always sufficient to differentiate and identify the person at issue, nor are they always necessary.

Given these problems with defining anonymity in terms of namelessness—specifically, that namelessness is neither a sufficient nor a necessary condition for anonymity; and conversely, that knowledge of a person's name is neither a necessary nor a sufficient condition for identification—anonymity should not be conceptualized in terms of the absence or presence of certain *types* of information. There is no single type of personal trait that is inherently identifying, nor is there any type of trait that can be removed to ensure anonymity.[113] Rather, the status of a trait as an identifying trait, or not, turns on two factors.

The first relevant factor is the *uniqueness* of the trait. A trait or set of traits must be unique in order to defeat anonymity. For example, if connecting the John Smith author to other facts about the book—such as year and place in which the author published it, the language in which he wrote it, etc.—results in a list of several different potential authors, the author will remain anonymous (though less so, in the sense that we will have increased the probability that it is one of a known set of people). Further, while uniqueness is a necessary condition for defeating anonymity, it is not itself sufficient. Take, for example, a random number assigned to a tissue sample in a research facility. This number is a unique trait not only of the tissue, but also of the tissue donor, who is "the person who donated tissue sample number X." But because the number is connected only with the tissue and its associated traits, it does not identify the donor. Identification requires more than individuation.

The second relevant factor is the extent to which a unique trait is *connected* to other relevant information.[114] For example, if I am looking for

[113] Here, my definition diverges from that of one of the few scholars who has focused on these questions about anonymity. See Gary T. Marx, What's in a Name? Some Reflections on the Sociology of Anonymity, 15 Info. Soc'y 99 (1999) (suggesting that anonymity is the absence of certain types of information).

[114] Here, I draw on Kathleen Wallace's idea of "noncoordinability of traits," though my definition departs from hers in significant ways discussed infra. See Kathleen A. Wallace, Anonymity, 1 Ethics & Info. Tech. 23, 24, 28 (1999).

a person in a crowd, and I know that the person has red hair, and that he is the only person with red hair, the connection between his red hair and the other information in my possession makes his red hair an identifying trait. Furthermore, and more generally, it is by virtue of such informational connections that a general fact about unidentified persons can become a fact about a specific person. Imagine, for instance, that I know that all the members of a group voted for the same candidate for president. If I do not know that my neighbor is a member of that group, his vote will be anonymous. But if I somehow connect him to that group, his vote will no longer be anonymous. Thus, whether a piece of information is a trait associated with a specific person turns on its connection to other information about that person. Information about groups, when combined with information that a specific person is a member of that group, becomes information about that person.

The problems of defining anonymity in terms of namelessness discussed above suggest that "identifying" a person can have both tangible and intangible dimensions—or in other words, that when we are trying to "pick someone out of the crowd," the crowd may consist of physical or purely informational persons. For example, imagine that I see the same person on my train commute every day for years without asking his name, and that I then see an anonymous photo of him on the news with a report that he is the subject of a police investigation. If the police want to physically locate this person, my knowledge of the train that he rides may be a fact that identifies him (in the relevant dimension, which is tangible); whereas if the police want to know his name, my knowledge of the train he rides may not identify him (in the relevant dimension, which is intangible). Thus, whether or not I "know who the person is in the photo" turns on the type of identification—the type of access to the person—that is sought.

Another example helps further clarify this point. Imagine two scenarios in which the police are trying to identify the person who committed a given crime. In the first, he is in hiding and the police want to arrest him; in the second, he is dead and the police have custody of his body. In the first scenario, many traditional identifiers (such as the suspect's name, personal history, social security number, and family members) will be irrelevant if the suspect has cut off all ties to his past, surgically altered his appearance, etc. In this case, the fact that the police know his name and history will not make him any less anonymous than he was made by the fact that they knew he committed the crime. If they saw

him on the street, he would be equally anonymous either way. In the second scenario, by contrast, the opposite might be the case. For example, if the police know that the person who committed the crime is dead, they might be primarily concerned with discovering the person's name, and knowledge of his physical location may be irrelevant. In short, to be anonymous is to be inaccessible in a given functional context.

Attention to this aspect of anonymity reveals why anonymity has often been associated with namelessness, and identification with being named. The reason why a name is often a good identifier is not because it is a unique trait (which it may or may not be), but rather because it is generally extensively connected with both tangible and intangible aspects of the person, which makes it likely that we will be able to "locate" the person in either dimension. For example, knowledge of a name can lead to a person's social security number, which can lead to bank records, mailing addresses, and the locations of recent credit card purchases—any of which might be the "locating" trait that is needed. Furthermore, this fact also explains why the value of names in this regard might be changing in the digital age, as other identifiers (such as online pseudonyms, and account numbers) are becoming extensively connected to many traits that may provide access to the person in a wide variety of relevant contexts.

Finally, because anonymity cannot be created by eliminating a type of information, but rather turns on connections and context, anonymity is always incomplete. Two points illustrate this lesson. First, the mere fact that we are confronted with an object or action that can be called "anonymous"—that we *know* is associated with an unknown person—means that we know a trait that might be an "identifier."[115] Take, for example, an anonymous book. The mere fact that we are confronted with a book that was written by someone means that we know something about that person. At the very least, we know that he or she wrote the book. In addition, we will likely know that he or she spoke the language in which the book is written. From the style of writing and word choice, we might also be able to identify the time period in which it was written, and perhaps even the place. In this way, the trait "he or she wrote this book" is a piece of information about the anonymous author that could, if sufficiently connected with other facts, be a trait that uniquely identifies the

[115] In this way, my account differs from G.T. Marx, who suggests that anonymity exists when no identifying traits are known. See Marx, supra note 113, at 100.

author. Second, the fact that the identity of someone is missing cannot itself be unknown. Anonymity presupposes a "knower" who knows that the identity of something is unknown. As Katherine Wallace notes: "A hermit may be 'nameless' or unknown but is not typically referred to as 'anonymous'; rather a hermit is an unrelated, socially disconnected agent."[116] To be anonymous, the hermit must be known as such. Because anonymity presupposes the existence of something that is known to be unidentified, and that thing will necessarily have features that are potential identifiers, anonymity is always incomplete. Thus, we should not define anonymity as the condition of being *unidentifiable*, as is often suggested in the literature,[117] but rather as the condition of being *unidentified* at a given time and place.

In sum, combining all of the above criteria, anonymity can be defined as a condition in which something associated with a person (such as an action, idea, object, etc.) is known only through traits that are not, without further information or investigation, unique and connected in a way that provides a relevant form of access to that person in a given context.[118]

C. Finding Anonymity in the Fourth Amendment

Recognizing the true nature of anonymity—and its relationship to privacy—reveals not only that there is a faulty premise at the core of the public exposure doctrine, but also, and more importantly, that courts should interpret the Fourth Amendment to protect "reasonable expectations of anonymity" on both formal and substantive grounds.[119]

---

[116] Wallace, supra note 114, at 24–25.

[117] See, e.g., id. at 23 ("[A]nonymity should be understood to mean, more broadly, nonidentifiability."); Peter West & Jacquelyn Burkell, Names, Nyms, Addresses and Reputations: The Experience of Anonymity in the Wired World, at 4 (2005) (unpublished manuscript) (available at http://idtrail.org/content/blogcategory/22/70/index.html) ("Someone who is 'anonymous' is indeed unnamed, but what matters is whether or not they *can* be named.").

[118] Although it is often said that "a person" can be anonymous, this wording can contribute to some conceptual confusion, in that "a person" is often conceptualized as an "individuated person," which is what an anonymous person is not. When we speak of an "anonymous person," we are really speaking of *something* associated with an individuated person (for example, a body, action, object, piece of information, etc.) that cannot be connected to him or her.

[119] In grounding this right to anonymity in the existing case law, my analysis will depart from the excellent work of Chris Slobogin on this topic. See Slobogin, supra note 81, at 217–18, 270–82 (arguing for a Fourth Amendment "right to anonymity" on the basis of an empirical survey of public perceptions of the "intrusiveness" of various police investigatory techniques, in which forms of public surveillance that do not constitute searches were ranked as

As a formal matter, courts should at the very least take reasonable expectations of anonymity into account when evaluating reasonable expectations of privacy. The reason for this is simple. Performing an action in public does not necessarily extinguish the privacy interests of the actor. As long as the action is anonymous, the disaggregation of the action and identity is maintained, thereby protecting the privacy of the actor. Take, for example, the Fourth Amendment interests of someone who donates a blood sample to research. If it is reasonable for the donor to expect that his sample will remain anonymous (perhaps because of promises made by the researchers, or because of the rules governing the institution), it will also be reasonable for him to expect that the information about him contained in the blood will remain private, despite the fact that this information is potentially accessible to others.[120] In this way, a reasonable expectation of anonymity can support a reasonable expectation of privacy, thereby bringing anonymity interests (and public facts) into the scope of the "privacy" protections recognized by the Fourth Amendment. Thus, even if a court were to insist on rigid formalism—and to limit the *Katz* test to the protection of "privacy" as traditionally conceived—its formalism would not allow it to reject the extension to anonymity.

Further, looking beyond the formality of the *Katz* test to its substance provides even stronger reasons to protect anonymity interests. For as Part I demonstrated, when the Supreme Court says "reasonable expectation of privacy," what it means is a reasonable expectation that a piece of personal information will remain unknown by others—a state of affairs that encompasses both "privacy" and "anonymity," as I have differentiated and defined them.

In fact, the Court has—on multiple occasions—explicitly stated that the Fourth Amendment is not merely concerned with privacy. For example, in a line from *Katz* that the Court has frequently reiterated, it stated that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion, but its protections go further,

being more intrusive than many types of searches—empirical data that Slobogin argues speaks to the core legal question of what "expectations of privacy society is prepared to recognize as reasonable").

[120] Of course there may be other ways in which his privacy with respect to this information is breached (for example, if the information is also contained in his medical records, and they are not anonymized); but with respect to the information as derived from the tissue, he can reasonably expect privacy.

and often have nothing to do with privacy at all."[121] Although the Court did not provide a detailed exposition of what it meant by this, it cited language from Justice Black's dissent in *Griswold v. Connecticut*, which stated that the Fourth Amendment protects a right to be left alone by the government that applies equally in public and in private.[122] This articulation of what the Fourth Amendment protects—a right to be left alone in public and in private—comes from another frequently reiterated line of *Olmstead v. United States*, where Justice Brandeis dissented from the majority's holding that wiretapping was not a Fourth Amendment violation absent physical trespass to the home. He wrote: "The makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[123]

While the Court has not explicitly characterized this interest in being "left alone in public" as an interest in "anonymity," a review of the Fourth Amendment case law post-*Katz* reveals that many cases that have been nominally about reasonable expectations of privacy have actually been about reasonable expectations of anonymity.

The Court's recognition that the Fourth Amendment protects against intrusions into one's anonymity can be seen most clearly in *Hiibel v. Sixth Judicial District Court of Nevada*,[124] where the Supreme Court addressed a Fourth Amendment challenge to a state statute that allowed the police to arrest a suspect who refused to identify himself in the course of an investigatory stop. The Court held that the statute did not violate the Fourth Amendment, but did implicate it. Specifically, the Court held that compelled identification was only constitutional in "the course of a valid *Terry* stop," and further, that "an officer may not arrest a suspect for failure to identify himself if the request for identification is not reasonably related to the circumstances justifying the stop."[125] Thus, the Court

[121] Katz v. United States, 389 U.S. 347, 350 (1967) (emphasis added); see also, e.g., Soldal v. Cook Cnty., 506 U.S. 56, 65 (1992) ("We thus are unconvinced that any of the Court's prior cases supports the view that the Fourth Amendment protects against unreasonable seizures of property only where privacy or liberty is also implicated.").

[122] *Katz*, 389 U.S. at 350 n.4 (quoting Griswold v. Connecticut, 381 U.S. 479, 509 (1965) (Black, J., dissenting)); see also, e.g., Spencer v. City of Bay City, 292 F. Supp. 2d 932, 945 (E.D. Mich. 2003) ("[T]he right to be left alone in public places ranks high on the hierarchy of entitlements that citizens in a free society have come to expect—at least in the context of citizen-police encounters—and one that is protected by the Fourth Amendment.").

[123] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[124] 542 U.S. 177 (2004).

[125] Id. at 188.

recognized that the Fourth Amendment protects a suspect's interest in remaining anonymous. The fact that this interest in anonymity can be outweighed by competing government interests—in this case, the same interests that allowed the police to temporarily seize the suspect for the *Terry* stop[126]—does not diminish but rather reinforces the fact that it is an interest protected by the Fourth Amendment.[127]

The same lesson can be found in a set of Supreme Court and circuit court cases addressing Fourth Amendment challenges to the mandatory DNA testing of arrestees, convicts, and parolees. The courts have uniformly rejected these challenges, holding that the practice does not violate a reasonable expectation of privacy. In reaching this conclusion, all of the courts have reasoned that this type of testing reveals nothing more than these persons' identities, and that given their status in the criminal justice system, they have no reasonable expectation of privacy in their identities. This rationale is stated most concisely by the U.S. Court of Appeals for the Second Circuit, which explained that "the DNA profile derived from the offender's blood sample establishes only a record of the offender's *identity*" and "a probationer's *expectation of privacy in his or her identity* is severely diminished."[128] While this logic has been widely criticized on substantive grounds,[129] what is relevant for my purposes is one of its formal features. Because "privacy of identity" is the same as "anonymity," these cases actually hold that there is no Fourth Amendment violation because people whose identities are already known to the criminal justice system have *no reasonable expectations of anonymity*.

Of course, the "best reading" of an area of case law will often not fit all of the cases. As case law develops over time in a manner that inevitably leads to some disorder, a coherent theory of the law will necessari-

[126] Id. at 185 ("To ensure that the resulting seizure is constitutionally reasonable, a *Terry* stop must be limited. The officer's action must be 'justified at its inception, and . . . reasonably related in scope to the circumstances which justified the interference in the first place.'" (omission in original)).

[127] See also Brown v. Texas, 443 U.S. 47, 53 (1979) (holding that a state may not make it a crime to refuse to provide identification on demand in the absence of reasonable suspicion).

[128] United States v. Amerson, 483 F.3d 73, 85, 86 (2d Cir. 2007) (emphases added). The same logic was used by the Supreme Court, see Maryland v. King, 133 S. Ct. 1958, 1978–80 (2013), and other circuits, see, e.g., Jones v. Murray, 962 F.2d 302, 306 (4th Cir. 1992) (explaining that the identity of an arrestee "becomes a matter of legitimate state interest and he can hardly claim privacy in it").

[129] For an excellent critique, see *King*, 133 S. Ct. at 1980 (Scalia, J., dissenting).

ly regard some parts of the law as mistaken or misconceived.[130] In order to bring coherence to the body, the theory must be able to explain how and why this is the case. And in this regard, my argument about the best reading finds additional support in a set of Supreme Court cases involving 5-4 splits.

Of particular relevance to my argument are the dissenting opinions in the Supreme Court cases that established the public exposure doctrine, all of which were decided on 5-4 lines.[131] Take, for example, the dissenting opinion of Justice Powell (joined by Justices Brennan, Marshall and Blackmun) in *California v. Ciraolo*, where the Court held that aerial observation of the fenced-in curtilage of a home did not constitute a search under the Fourth Amendment.[132] In explaining why the public exposure doctrine should not apply to such surveillance—in explaining what the Court was missing—Justice Powell pointed not to privacy, but to anonymity:

> Travelers on commercial flights, as well as private planes used for business or personal reasons, normally obtain at most a fleeting, *anonymous*, and nondiscriminating glimpse of the landscape and buildings over which they pass. The risk that a passenger on such a plane might observe private activities, and might *connect those activities with particular people*, is simply too trivial to protect against.[133]

Thus, my reading of the case law matches that of the four Justices in this case who concluded that surveillance can violate the Fourth Amendment by virtue of violating a defendant's reasonable expectations of anonymity.[134]

---

[130] See Ronald Dworkin, Taking Rights Seriously 116–18 (1978).

[131] See, e.g., Florida v. Riley, 488 U.S. 445, 456–57 (1989) (Brennan, Marshall & Stevens, JJ., dissenting); id. at 467 (Blackmun, J., dissenting); Dow Chem. Co. v. United States, 476 U.S. 227, 248–52 (1986) (Powell, Brennan, Marshall & Blackmun, JJ., concurring in part and dissenting in part); California v. Ciraolo, 476 U.S. 207, 215–16, 223–26 (1986) (Powell, Brennan, Marshall & Blackmun, JJ., dissenting).

[132] 476 U.S. 207 (1986).

[133] Id. at 223–24 (Powell, Brennan, Marshall & Blackmun, JJ., dissenting) (emphasis added) (footnote omitted).

[134] Likewise, in *Nader v. General Motors Corp.*, Justice Breitel spoke in terms of anonymity and disconnectedness in arguing that the majority failed to recognize an important set of privacy interests under tort law:

> [I]t does not strain credulity or imagination to conceive of the systematic 'public' surveillance of another as being the implementation of a plan to intrude on the privacy of another. Although acts performed in 'public', especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may neverthe-

In addition, and even more importantly, my reading is supported by the recent GPS tracking case of *United States v. Jones*, which reveals that a majority of the Court believes that the public exposure doctrine is limited in previously unarticulated ways.[135] The question in *Jones* was whether the police had violated the Fourth Amendment when they installed a GPS on the defendant's car and monitored his public movements for twenty-eight days. All of the members of the Court agreed that the Fourth Amendment had been violated, but they disagreed on the reason. The majority opinion held that the constitutional problem was the *installation* of the GPS, on the grounds that it involved trespass onto the defendant's private property—the pre-*Katz* Fourth Amendment standard.[136]The concurring opinion of Justice Alito (joined by Justices Ginsburg, Breyer, and Kagan), by contrast, found that the problem was the *monitoring* of the defendant's public movement, on the grounds that this violated the *Katz* test.[137] Finally, the concurring opinion of Justice Sotomayor, who joined the majority, expressed agreement with Alito's view, but explained that it posed difficult questions about the precise limits of the public exposure and third party doctrines that she thought were best postponed to a future case.[138]

Thus, the best reading of *Katz* and its progeny must be able to explain when and why the public exposure doctrine does not apply to movements in public—to explain this newly articulated limit on its scope. And as is demonstrated above, my reading provides such an explanation. Furthermore, as Part III will argue in depth, such an explanation cannot be adequately articulated in terms of the concept of privacy. At this point, I will merely note that this lesson seems to have been recognized by Chief Judge Kozinski when he dissented from the Ninth Circuit's de-

> less be invaded through extensive or exhaustive monitoring and cataloguing of acts normally *disconnected* and *anonymous*.

255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring in the judgment) (emphases added). Further, in the Fourth Amendment GPS tracking case that later became *United States v. Jones*, 132 S. Ct. 945 (2012), the opinion of the D.C. Circuit relied on this concurrence: "A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'" United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (quoting *Nader*, 255 N.E.2d at 772 (Breitel, J., concurring in the judgment)).

[135] *Jones*, 132 S. Ct. at 945.

[136] Id. at 948–49.

[137] Id. at 958–60 (Alito, Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

[138] Id. at 954–57 (Sotomayor, J., concurring).

nial of rehearing en banc in a GPS tracking case. In arguing that GPS tracking can implicate the Fourth Amendment—that the public exposure doctrine does not apply to *all* movements in public—Judge Kozinski explained: "You can *preserve your anonymity* from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to be followed."[139] In other words, someone can have a reasonable expectation of anonymity when moving in public, and in such cases, the fact that the person is making these movements will not be exposed. It is for this reason that GPS tracking is not automatically subject to the public exposure doctrine and can constitute a search under the Fourth Amendment.

Finally, it is worth noting in conclusion that while my argument is based on the fact that the Court has adopted a non-normative conception of privacy, a normative conception might support the same conclusion. This would, of course, depend on the way in which the normative aspects of privacy were defined. For example, if the Supreme Court had concluded that the Fourth Amendment's protections of privacy were only meant to protect the government from intruding on "intimate" matters, one might argue that the amendment's protections should be limited to places or information that could be involved in fostering or maintaining this intimacy. In this case, the best reading of the cases might not support extending the Fourth Amendment to protect anonymity in public. But it seems that a better normative reading of the Fourth Amendment might extend to anonymity. For, as other scholars have argued, protections of anonymity in public places (like protections of privacy in the home) can be integral to the flourishing of not only an individual's dignity, individuality, and autonomy, but also a free and open society.[140]

[139] United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (emphasis added).

[140] See Richard A. Wasserstrom, Privacy: Some Arguments and Assumptions, *in* Philosophical Dimensions of Privacy: An Anthology 317, 325–27 (Ferdinand David Schoeman ed., 1984); Jeffrey H. Reiman, Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, 11 Santa Clara Computer & High Tech. L.J. 27, 41–42 (1995); see also United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting) ("Authority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed. Were third-party bugging a prevalent practice, it might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life.").

III. REASONABLE EXPECTATIONS OF ANONYMITY

The above analysis not only reveals why the Fourth Amendment should protect reasonable expectations of anonymity as a general matter, but also provides the tools needed to answer difficult and pressing questions about specific new techniques of data collection and analysis. To demonstrate these applications, this Part focuses on two relatively new surveillance practices. The first is a form of genetic identification known as "familial searching," in which a criminal DNA database is used to identify potential suspects who do not have profiles included in the database, but happen to be genetic relatives of included offenders. The second is the use of tools such as biometric-equipped video cameras, GPS, and the metadata from cell phone calls to conduct long-term locational tracking of people's movements in public.

While both of these practices have faced significant criticism in the privacy scholarship, and there is language in judicial opinions questioning their legitimacy, these concerns have not been well grounded in the Fourth Amendment. The missing foundation is provided by the concept of "reasonable expectations of anonymity," which has two core payoffs. First, it provides courts with a principled standard that not only reveals the otherwise-unrecognizable ways in which these new surveillance practices implicate the Fourth Amendment, but also is capable of differentiating seemingly similar practices that do not. Second, it helps courts apply the Fourth Amendment in ways that bring us closer to realizing its substantive promise. These are the two core arguments of this Part.

Before developing these arguments, however, it is perhaps worth highlighting in advance that this Part does not address the question of whether familial searching and long-term surveillance technologies are necessarily unconstitutional and must be removed from the set of tools available to the police. Rather, this Part only addresses the foundational question of whether they implicate the Fourth Amendment—of whether they constitute a search that must be justified. The further question of what procedural safeguards could be used to make their use reasonable, and thereby constitutional, is outside the scope of this Article, though a few brief suggestions along these lines will be offered.

A. Genetic Identification

This Section demonstrates that understanding the relationship between anonymity and privacy uncovers and provides insights into the le-

gal interests that are threatened by a technique of genetic identification known as "familial searching." As is explained in more detail below, this is a technique of running a search in a criminal DNA database that in effect expands the database to include profiles for persons who do not meet the legal criteria for inclusion, but who happen to be genetically related to included "offenders."[141] A variety of strong normative arguments for restricting or rejecting this search technique have been developed in the scholarly literature,[142] and there are dicta in some judicial opinions implying concern about its use.[143] However, neither courts nor scholars have been able to explain how this technique implicates the Fourth Amendment, as the technique does not in and of itself discover private facts. To explain the constitutional problem, courts and scholars need to think in terms of anonymity rather than privacy. What this approach reveals is that familial searching effectively creates "virtual profiles" in the DNA database for people who are unknown to the criminal justice system, thereby violating reasonable expectations of genetic anonymity that courts have implicitly recognized—and should now explicitly recognize—as protected interests under the Fourth Amendment.

1. The Insufficiency of Privacy

a. The Nature of Familial Searching

DNA profiling is a process in which a biologically unique set of numbers is derived from an individual's DNA. These numbers are created by analyzing specific regions of DNA that have varying numbers of a given repeated genetic sequence; these repeats are located in portions of the

[141] Although these databases increasingly include arrestees, I will for the sake of clarity follow the convention of referring to them as included "offenders."

[142] See Erin Murphy, Relative Doubt: Familial Searches of DNA Databases, 109 Mich. L. Rev. 291 (2010); Natalie Ram, Fortuity and Forensic Familial Identification, 63 Stan. L. Rev. 751 (2011); Sonia M. Suter, All in the Family: Privacy and DNA Familial Searching, 23 Harv. J.L. & Tech. 309 (2010).

[143] For example, in a recent Supreme Court case upholding a statute requiring DNA profiling of arrestees, the Court emphasized that familial searching was prohibited under the statute. Maryland v. King, 133 S. Ct. 1958, 1967 (2013); see also Haskell v. Harris, 669 F.3d 1049, 1079 (9th Cir. 2012) (Fletcher, J., dissenting) (expressing concern about the possibility of DNA being used for familial searching in the future); United States v. Mitchell, 652 F.3d 387, 409 n.19 (3d Cir. 2011) (emphasizing that DNA database software is "not designed for intentional familial searches" in rejecting defendant's attempt to distinguish DNA from fingerprints); Boroian v. Mueller, 616 F.3d 60, 69–70 (1st Cir. 2010) (acknowledging familial privacy concerns arising from DNA database searches, but concluding that the database software as it currently stands does not pose a threat).

DNA that have no known function and thus do not provide any other relevant biological information about the person.[144] As a tool of criminal law, DNA profiling was originally only used for sex offenders, but over time this expanded, and forty-nine states and the federal government now require DNA profiling for every convicted felon.[145] In addition, at least twenty-four states and the federal government have passed laws authorizing collection of DNA from arrestees as well.[146] In many of the states that take DNA samples upon arrest, the samples and profiles of individuals who are not ultimately convicted are not automatically destroyed; rather, the exonerated individuals must go through a lengthy process of requesting an expungement.[147] As of September 2014, the national database run by the FBI, which consists of state and federal records, contains 11,164,117 offender profiles and 2,026,761 arrestee profiles.[148]

Thus far, the legal challenges to DNA profiling have focused on the rights of the people being profiled. In resolving these challenges, courts have addressed whether it matters if the person being profiled is an arrestee, convict, or ex-convict;[149] whether it matters if the crime at issue is a violent or nonviolent felony;[150] and whether it matters if the government will maintain and run searches against the profiles indefinitely.[151] Controversially, courts have held that none of these factors changes the outcome of the constitutional analysis of DNA profiling.[152] They

[144] However, this does not mean that they have no function, and some studies are now questioning the conventional wisdom that they are "junk" DNA. See Elizabeth Pennisi, DNA Study Forces Rethink of What It Means to Be a Gene, 316 Science 1556, 1556–57 (2007).

[145] DNA Laws Database Topic Summaries, Nat'l Conference State Legislatures, http://test.ncsl.org/issues-research/justice/dna-laws-database-topic-summaries.aspx (last visited Nov. 13, 2014) [hereinafter DNA Laws Database Topic Summaries] (states); see also 28 C.F.R. § 28.12(b) (2012) (federal government).

[146] See sources cited supra note 145.

[147] See DNA Laws Database Topic Summaries, supra note 145.

[148] CODIS—NDIS Statistics, FBI, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics (last visited Nov. 13, 2014).

[149] See, e.g., United States v. Mitchell, 652 F.3d 387, 410–12 (3d Cir. 2011) (en banc) (upholding the suspicion-less collection of DNA samples from arrestees on the same grounds as felons).

[150] See, e.g., United States v. Amerson, 483 F.3d 73, 75 (2d Cir. 2007) (upholding the collection of DNA from individuals convicted of nonviolent crimes and sentenced only to probation).

[151] See, e.g., *Amerson*, 483 F.3d at 86 (upholding indefinite retention and use of DNA profiles for probationers and convicted felons).

[152] See supra notes 149–48.

have held that the government's acquisition of the DNA sample constitutes a search, but is constitutionally reasonable in all these cases.

The arrestees and offenders who are being profiled are not, however, the only people whose interests are implicated by the creation and use of DNA databases. Thus, there is an important question that has not yet been addressed by the courts. It is a question about the interests of persons who are not already known to the criminal justice system, but who are brought into the system through the use of a DNA database search technique known as "familial searching."

Unlike the standard technique of searching, which looks for exact matches between DNA found at crime scenes and the DNA of persons in the database, familial searching looks for partial matches in order to find genetic relatives of the person whose DNA is at the crime scene. This technique is generally used when a database search for a piece of crime-scene DNA does not turn up an exact match. In these cases, the police can follow up with a moderate- or low-stringency search that returns profiles matching some, but not all, of the genetic markers in the profile. The value of doing so is that these commonalities (depending upon how many there are and how rarely or frequently they occur at random in human populations) are more likely to be observed in relatives than in unrelated people. Studies suggest that if the database includes a genetic relative of the unidentified DNA suspect, and the search threshold is set widely enough, there is an 80–90% chance that this relative will be included in the list of results (which are likely to also include as many as twenty-four other people who are not in fact related to the unidentified suspect).[153] In this way, the relatives of all the included offenders who are partial matches become potential suspects for the police to consider.

The literature has identified a variety of normative concerns with this use of DNA databases, three of which are particularly strong. The first is well developed in the excellent work of Erin Murphy on this topic, who argues that familial searching creates a list of suspects "compiled on no other basis than that they, rather than the rest of the population with the same characteristics, happen to have kin in the offender database."[154] In doing so, it arbitrarily distinguishes between people who have relatives in the database, and those who do not.[155] Both groups of persons are

[153] Murphy, supra note 142, at 297–98.
[154] Id. at 338–39.
[155] Id. at 305.

equally nonincludable in the database as a matter of law, as seizing their blood and including their genetic profiles in the database would violate the Fourth Amendment.[156] Yet the former group is effectively included in the database as a product of "biological happenstance."[157] Thus, if a universal database is not considered justifiable, expanding the DNA database to include some non-offenders based on an arbitrary factor should be considered equally problematic.[158]

The second concern is that this arbitrary distinction between groups largely cuts along racial and ethnic lines, aggravating disparities in the criminal justice system.[159] The reason for this is that racial and ethnic minorities are significantly overrepresented in offender databases—a bias that is then amplified by familial searching. Hank Greely notes that under one estimate, "more than four times as much of the African-American population as the U.S. Caucasian population would be 'under surveillance'" if familial searching became widespread.[160] Further, if databases expand to include all arrestees (as many are), the result may be functionally indistinguishable from a universal DNA database for African Americans, but not other ethnic or racial groups.[161] While this disparate impact alone is insufficient to implicate the Equal Protection Clause, as it is not the result of discriminatory purpose or intent, it is problematic under many theories of social justice.[162]

The third concern is that the way in which familial searching has been implemented thus far "subverts democratic accountability."[163] The problem, as Natalie Ram argues, is that the adoption of familial searching has "largely been effectuated through inaccessible lab policies, and rarely through means in which the public may actively participate," which means that it has widened "the genetic net without statutory amendment

[156] See Friedman v. Boucher, 568 F.3d 1119, 1130 (9th Cir. 2009).

[157] Ram, supra note 142, at 789.

[158] Murphy, supra note 142, at 313.

[159] See, e.g., Henry T. Greely et al., Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin, 34 J.L. Med. & Ethics 248, 258–59 (2006) (estimating disparate impact of partial DNA matching on African American families compared to Caucasian families); Murphy, supra note 142, at 321–25 (explaining how the current DNA collection and database systems exacerbate racial inequities and biases in the criminal justice system).

[160] Greely et al., supra note 159, at 259.

[161] See D.H. Kaye & Michael E. Smith, DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage, 2003 Wis. L. Rev. 413, 455–56.

[162] See Greely et al., supra note 159, at 259.

[163] Ram, supra note 142, at 794.

or, in most instances, public knowledge."[164] It has widened the effective size of databases, the types of testing conducted on them, and thus the types of information revealed. Thus, the "relative lack of public knowledge about these policies and the near-total lack of public oversight in their promulgation sets the adoption of partial matching apart from previous database expansions" in normatively relevant ways.[165]

b. Privacy-Based Critiques

While scholars have identified a variety of strong normative arguments for restricting or rejecting the use of familial searching, grounding these objections in the law has been difficult. While most agree that if there is a legal problem, it is likely to be found in the restrictions of the Fourth Amendment, the arguments that the practice violates the Fourth Amendment have been less compelling than the normative arguments. The reason for this, I will argue, is that they have focused on privacy rather than anonymity.

Privacy-based critiques of familial searching generally start with the fact that courts have held that mandatory genetic profiling *does* constitute a Fourth Amendment search, but that it is reasonable and thus constitutional. Most recently, the Supreme Court upheld the genetic profiling of arrestees under a balancing test: It held that arrestees have diminished expectations of privacy, that states have strong interests in accurately identifying arrestees, and that the latter outweighs the former.[166] Setting aside questions about the strength of this justification,[167] critics of familial searching argue that what is important here is that this justification does not apply to the arrestees' relatives—people whose privacy expectations are not diminished, and for whom the state has no

[164] Id.

[165] Id. A fourth concern raised by Erin Murphy, which I think is mistaken as a descriptive matter, is that the use of familial searching embodies "presumptions that our constitutional and evidentiary rules have long endeavored to counteract" including "guilt by association . . . and even biological determinism." Murphy, supra note 142, at 304. While it is true that these presumptions would support the use of familial searching, there is little evidence that they are actually behind its use, which can be justified on scientifically valid grounds. A fifth argument advanced by Murphy, which I think is descriptively accurate but deserves less normative weight, is that familial searching can disrupt families in significant ways. See id. at 319–20 (arguing that it can "deepen painful rifts within strained familial relationships" by bringing unwanted attention to innocent family members, or by turning those who are in the database into "involuntary 'genetic informants'" on guilty family members).

[166] See Maryland v. King, 133 S. Ct. 1958, 1978–80 (2013).

[167] For a strong critique, see id. at 1986–89 (Scalia, J., dissenting).

special interest in forensic identification. Erin Murphy, for example, argues that familial searching violates the Fourth Amendment on the grounds that it exploits "databases compiled on the premise of lessened privacy of offenders to access the fully protected DNA profiles of relatives."[168] Furthermore, she suggests that because familial searching—unlike standard searches—produces many incorrect hits, "the potential harm to relatives exceeds that of even the actual offenders."[169]

While this critique has intuitive appeal, it faces a problem in that it rests on the premise that the justifications for DNA profiling need to apply to familial searching—a premise that has not been adequately established. The problem is that familial searching may not even constitute a Fourth Amendment event for which such a justification is required. The determinative question here is whether familial searching should be treated as nothing more than using an existing database, or whether it should instead be treated as creating new profiles.

If familial searching is best understood as a form of database use, then the weight of the case law suggests that it does not constitute a Fourth Amendment event. There are two reasons for this. First, courts have generally held that running an analysis in a database is not a search.[170] Second, the Supreme Court's holding that DNA profiling constitutes a Fourth Amendment search relied on the fact that the collection of DNA involved bodily intrusion (in that case, a cheek swab), which is not present in the case of familial searching.[171]

If, on the other hand, familial searching is best understood as creating new profiles, one might argue that it constitutes a Fourth Amendment

[168] Murphy, supra note 142, at 336.

[169] Id. at 317. She further notes:

> If familial searching is to be allowed, a relative would be wise to volunteer a genetic sample (and thus be more readily excluded) rather than run the risk of repeated requests for samples that ultimately prove not to match. But these innocent persons should not have to make such a strategic election when they are, like all other persons, legally entitled to the full privacy protections of the Fourth Amendment.

Id.

[170] See, e.g., Johnson v. Quander, 440 F.3d 489, 498 (D.C. Cir. 2006) ("[A]ccessing the records stored in the CODIS database is not a 'search' for Fourth Amendment purposes."). But see United States v. Weikert, 504 F.3d 1, 16–17 (1st Cir. 2007) ("[I]t may be time to reexamine the proposition that an individual no longer has any expectation of privacy in information seized by the government so long as the government has obtained that information lawfully . . . . [T]here may be a persuasive argument on different facts that an individual retains an expectation of privacy in the future uses of her DNA profile.").

[171] *King*, 133 S. Ct. at 1968–69.

event. The reason for this is that the Supreme Court has held that taking a blood sample and analyzing that sample are two separate searches under the Fourth Amendment, each implicating different expectations of privacy. The Court has explained that the "physical intrusion, penetrating beneath the skin, infringes an expectation of privacy that society is prepared to recognize as reasonable" related to "the security of one's person," while "[t]he ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested employee's privacy interests."[172] Following this logic, several federal courts of appeals have held that the same applies to DNA profiling on the grounds that it also reveals personal information.[173] While all of these cases involved a physical search (obtaining the DNA) that is not present in the case of familial searching, none of these cases suggested that this was necessary. Rather, they relied on the fact that the blood or DNA analysis revealed data about the individual. Thus, when framed in this way, the core constitutional question becomes whether familial searching reveals private information about the relatives of the included offenders.

In arguing that familial searching does reveal private information about relatives, some scholars have pointed to the fact that it makes the relatives targets of police investigation. For example, Natalie Ram notes that familial searching "makes otherwise nonincluded relatives targets of investigation," and that while this "generates broad possibilities for investigation, it also inherently identifies many spurious connections to offenders, exacerbating the invasion of privacy."[174] But there is a problem with this line of critique, for although such privacy invasions are undoubtedly real, they do not implicate privacy interests that the Fourth Amendment protects. The reason for this is that the invasion is not caused by the familial search itself, but rather by the police's use of the results in creating and investigating a suspect list. And the Fourth Amendment does not protect people from being the subject of mistaken suspicion, even if it causes the serious intrusions into private life that ac-

[172] Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 616 (1989).

[173] See, e.g., United States v. Davis, 690 F.3d 226, 246 (4th Cir. 2012) ("[T]he extraction of DNA and the creation of a DNA profile result in a sufficiently separate invasion of privacy that such acts must be considered a separate search under the Fourth Amendment even when there is no issue concerning the collection of the DNA sample."); Nicholas v. Goord, 430 F.3d 652, 670 (2d Cir. 2005) ("The second intrusion to which offenders are subject is the analysis and maintenance of their DNA information in New York's database. This intrusion may be viewed either as a search or as a seizure.").

[174] Ram, supra note 142, at 791.

company a police investigation. As David Kaye notes: "The individual interest in being free from falsely incriminating trawls is legitimate enough, but it too does not count in the Fourth Amendment calculus . . . . For better or worse, the Fourth Amendment . . . does not protect against mistaken inferences from the fruits of a search."[175]

Furthermore, the same is true of accurate inferences that emerge from a police investigation, which others have relied on in arguing that familial searching violates reasonable expectations of privacy. For example, inquiries based on familial searching can reveal very private facts—such as the fact that two members of a family are not genetically related in the way that was thought (for instance, that a son is not the genetic child of his father). However, as with mistaken suspicion, the Fourth Amendment does not protect against accurate discoveries of private information in the course of police work that does not itself constitute a search.[176]

Thus, if familial searching implicates a Fourth Amendment interest, it must be because of some private information that is revealed by the technique itself, and not the subsequent police investigation. One possible contender for this can be found in Erin Murphy's claim that familial searching implicates the relative's privacy by exposing her genetic information. She argues that "the relative has a protected right not to have her own genetic information exposed, if you will, by the fact of her kin's conviction."[177] In making this argument, Murphy relies on an analogy to the joint privacy interests held by co-occupants of a residence, where one occupant's consent to police entry cannot vitiate the other's denial of consent. Murphy suggests that we could likewise conclude "that the convicted offender's diminished privacy cannot in turn diminish the privacy of his or her relatives."[178] But the co-occupant example is inapposite in several key ways. Unlike with two people who share a residence, it cannot be the case that DNA profiling requires the consent of all per-

[175] David Kaye, DNA Database Trawls and the Definition of a Search in *Boroian v. Miller*, 97 Va. L. Rev. In Brief 41, 47–48 (2011).

[176] Here, I set aside discoveries made through Y-STR analysis, which is a method of *confirming* a familial match. It uses the stored blood sample of the offender to conduct a more definitive Y-chromosome analysis that can confirm male biological links between men. In doing so, this Y-chromosome analysis can reveal intimate secrets of familial relationships such as the identities of biological parents in a closed adoption, a sperm or egg donor's identity, or misattributed paternity. Because this information derives from the analysis of the DNA, it arguably fits more closely within the definition of a search established by the Supreme Court's blood and urine testing cases.

[177] Murphy, supra note 142, at 336.

[178] Id.

sons who share a genetic profile; otherwise, an identical twin would be able to prevent the government from profiling his twin.[179] In addition, the co-occupancy example involves issues of conflicting consent not present in the DNA case, where the government can compel profiling without consent.

Furthermore, setting aside the strength of analogy to co-occupancy, there are three even deeper problems with this line of argument, which together reveal the core of the problem with privacy-based arguments against familial searching. The first problem is that the DNA profiles in the databases only contain *noncoding* genetic information (information that does not reveal any biological facts about the person), and for this reason, the familial searching of the database can likewise only provide noncoding information about unincluded relatives.[180] The second problem is that the limited noncoding information that is revealed by familial searching is not specific to any one relative, but rather is shared by *a group*, and it is moreover *probabilistic*: All that is known is that one of the relatives of the person in the databank might be the source of a piece of forensic DNA. The third problem is that the group information that is discovered is about a group of *unidentified* persons. To learn the identities of these persons, the police must use publicly available knowledge about the family tree of the person whose DNA profile is included in the databank. It is only by virtue of this public information that they can discover the identity of the person about whom they have information. Recognizing these problems with the privacy-based arguments is instructive, however, in identifying an interest that is fundamentally at stake in familial searching: an interest in anonymity.

2. Seeing the Constitutional Problem

To see the Fourth Amendment interests that are implicated by familial searching, it is helpful to start by returning to a point that I mentioned above: The creation of a DNA profile is itself a Fourth Amendment search. Thus far, most of the critical scholarship has relied on this point

[179] Natalie Ram makes an even stronger suggestion, noting that the fact that we share our genetics might mean "that no one has an expectation of privacy in genetic information, rather than that we have such expectations in the DNA of others as well as our own." Ram, supra note 142, at 793.

[180] However, as discussed supra note 176, subsequent Y-STR analysis can reveal private information. Further, there are some studies that question whether these regions are truly noncoding. See Pennisi, supra note 144, at 1556.

in making privacy-based arguments against familial searching. The basic strategy of these arguments is to claim that a familial search results in the same privacy invasions as the creation of a DNA profile and is thus also a search, but without the necessary constitutional justification. I have argued that this strategy is misguided, as there do not appear to be any Fourth Amendment privacy interests that are implicated by familial searching. However, returning to this starting point offers an alternate path forward—one that is based not on the private information that is revealed by the technique, but rather on the technique itself.

The core constitutional problem with familial searching derives from the simple fact that the technique effectively creates "virtual" profiles for all the relatives of included offenders and maintains them in the database. Further, these virtual profiles can be identical to real profiles in practice—especially when the police are trying to match an incomplete piece of DNA from a crime scene. In these cases, the police will likely only be able to find a partial match to an included offender, even if it is his DNA at the crime scene; and this partial match will be functionally identical to the partial match that they obtain when they perform a "familial search" in the database. There will be no functional difference between the actual and the virtual profile.[181]

There is, however, an important legal difference in the interests of the persons who are profiled in these two ways: The virtual profiles belong to persons who are not already known to the criminal justice system, whereas the actual profiles belong to persons who have been arrested or convicted. For this reason, these two groups of people have very different anonymity interests. Whereas arrestees and offenders do not have a reasonable expectation of anonymity with respect to the state, their relatives do, and it is these interests that are implicated by the creation of the virtual profile.

In response to this argument, one might claim that even if the relatives have a reasonable expectation of anonymity, this interest is not actually implicated by familial searching. This claim could be based on the argument I advanced above (in response to privacy-based theories) that familial searching does not itself reveal the names of relatives. The police can only learn the names associated with the virtual profiles by us-

[181] There is just one difference between these "virtual profiles" and the profiles of included offenders: An offender profile is complete and can therefore provide a complete match with crime scene DNA, whereas these "virtual profiles" are incomplete (they are based on a partial match) and can therefore only provide partial matches with crime scene DNA.

ing publicly available knowledge about the family tree of the person whose DNA profile is included in the databank. For example, if a familial search produces a partial match with John Smith, the police will need to look outside the database to learn the names and addresses of John Smith's relatives. On these grounds, one might argue, the anonymity of the relatives remains intact even after the familial search.

The problem with this rejoinder, however, is that anonymity is not the same as namelessness, nor is it a binary state (as is discussed in depth in Section II.B).[182] For these reasons, the fact that someone remains nameless does not mean that he remains anonymous, nor does the fact that he remains anonymous mean that no anonymity has been lost. Rather, as I argued above, anonymity is broken down through the connections of facts about a person that enables him or her to be "found" in the relevant context. And that is precisely what familial searching achieves. The familial search connects the crime scene DNA sample to an offender profile in the database, connects this offender profile to a "virtual profile," and then connects this virtual profile to the relatives of the offender. Through the series of connections created by the familial search, the anonymity of the relatives breaks down; they are rendered "findable" by their genetics.

Furthermore, and most importantly, the reasonable expectations of anonymity of these relatives who have not been arrested have been implicitly recognized as Fourth Amendment interests by courts addressing the constitutionality of DNA profiling. As discussed in Section II.C,[183] the Supreme Court and courts of appeals cases that have upheld the profiling of arrestees and convicts have implicitly done so on the grounds that these persons do not have reasonable expectations of anonymity with respect to the state. As the Second Circuit stated most directly, "[T]he DNA profile derived from the offender's blood sample establishes only a record of the offender's *identity*" and this person's "*expectation of privacy in his or her identity* is severely diminished."[184] To say that someone has no reasonable "expectation of privacy in his or her

[182] See supra notes 110–17 and accompanying text.

[183] See supra notes 119–38 and accompanying text.

[184] United States v. Amerson, 483 F.3d 73, 85–86 (2d Cir. 2007) (emphases added). The same logic was used by the Supreme Court, see, e.g., Maryland v. King, 133 S. Ct. 1958, 1978 (2013) ("[U]nlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy."), and other circuits, see, e.g., Jones v. Murray, 962 F.2d 302, 306 (4th Cir. 1992) (noting that the identity of an arrestee "becomes a matter of legitimate state interest and he can hardly claim privacy in [his identity]").

identity" is merely another way of saying that he or she has no reasonable "expectation of anonymity." Thus, courts have implicitly held that it is expectations of anonymity that are relevant when evaluating the constitutionality of creating databases of genetic identifiers—which in retrospect should not be surprising given that identifiers first and foremost implicate anonymity rather than privacy. It is only because anonymity and privacy have been conflated that this point has been obscured.

In sum, differentiating between anonymity and privacy reveals an oversight in the critical literature on familial searching, as well as the true way in which it implicates the Fourth Amendment. The problem with familial searching is not that it breaches the reasonable expectations of privacy of the relatives of included offenders, but rather that it breaches their reasonable expectations of genetic anonymity—expectations that courts have implicitly recognized, and should now explicitly recognize, as protected interests under the Fourth Amendment.

B. Locational Surveillance

This Part has thus far demonstrated that understanding the difference and relationship between anonymity and privacy illuminates an important and viable set of Fourth Amendment interests that has gone unrecognized by courts and scholars. This Section identifies additional ways in which my analysis reveals significant oversights in Fourth Amendment law—oversights that are most apparent in the context of long-term locational tracking.

As noted in the Introduction, technologies that allow for low-cost and long-term locational tracking are becoming increasingly widespread. For example, cell phone service providers are storing the locational data of every call that they connect, allowing for the retroactive identification of the locations and movements of anyone using a cell phone. Roadside cameras are amassing millions of digital records by logging every car that passes them, allowing the police to identify the location and movement of a given vehicle based on its license plate number.[185] And video surveillance cameras equipped with facial recognition software are being developed to scan crowds in public spaces to identify and track individuals based on their unique biometric features.[186]

[185] ACLU, supra note 3, at 7 (reporting results of FOIA requests).
[186] Savage, supra note 2.

Like the use of familial searching, the use of these forms of locational surveillance has been extensively criticized in the privacy literature and questioned in some judicial opinions,[187] but this criticism has generally lacked a strong Fourth Amendment foundation.[188] While concurring opinions in the recent case of *United States v. Jones* revealed that five members of the Supreme Court think that some forms of long-term location tracking can implicate the Fourth Amendment,[189] these opinions did not provide an explanation of when and why the public exposure doctrine does not apply to movements in public, nor did they articulate a rule or standard that could be used to differentiate between cases of long-term surveillance.

This Section first demonstrates that my analysis of the relationship between anonymity and privacy solves the puzzles left open by the *Jones* concurrences—one that cannot be answered by reference to the existing privacy-based framework. What is needed is my analysis of the place of anonymity in the Fourth Amendment. This approach provides a standard that cannot only explain when and how public locational tracking constitutes a search, but also differentiates cases of surveillance that do not. In addition, it reveals previously unrecognized ways in which the secrecy of our personal information can be maintained in public places, helping bring us closer to the promise of the Supreme Court's teaching that "the Fourth Amendment protects people, not places."[190]

1. The Insufficiency of Privacy and Mosaics

The key challenge to bringing long-term location-tracking technologies under the scope of the Fourth Amendment is explaining how they

[187] Chris Slobogin argues convincingly that generalized public surveillance is normatively objectionable on the grounds that it intimidates those engaging in political expression, inhibits public movement, affects one's personality, and accelerates normalization—and that in doing so, it implicates a variety of constitutional values other than the Fourth Amendment. See Slobogin, supra note 81, at 252–67. In addition, he argues that the Supreme Court should recognize a Fourth Amendment right to public anonymity that would be implicated by public surveillance. Id. at 217, 299–300. However, this argument is not based in current doctrine, but rather on an empirical survey of public perceptions of the "intrusiveness" of police investigatory techniques, in which public surveillance was generally ranked higher than other techniques that constitute searches. Id. at 267–82.

[188] The exception is when the installation of the tracking device constitutes a trespass. See United States v. Jones, 132 S. Ct. 945, 948–50 (2012).

[189] Id. at 954–55 (Sotomayor, J., concurring); id. at 964 (Alito, Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

[190] Id. at 351.

differ from predecessor techniques that are not unconstitutional. Compare, for example, the tracking of a person's movement for a day by undercover police, and the tracking of a person's movements for weeks using biometric video tracking. Given that the former practice is not a Fourth Amendment search, a question that has recently been the subject of significant attention is whether the latter practice can be differentiated on legally relevant grounds—whether the multi-week information is not publicly exposed in the same way. The following analysis will show that the existing Fourth Amendment framework is ultimately unable to differentiate the practices in a legally satisfying manner.

Under a privacy-based framework, there are two seemingly promising ways of establishing that the locational data that are collected by long-term surveillance technologies differ from the data that are collected by traditional surveillance techniques and thus should not fall under the scope of the public exposure doctrine.[191]

One way of trying to do so is by reference to the Supreme Court's distinction between technologies that are sense-augmenting and those that are extrasensory—the former being presumptively excluded from the constitutional definition of a search, and the latter being presumptively included.[192] For example, one could argue that computerized technologies that allow for remote, long-term surveillance do not merely augment the senses normally used in surveillance, but rather replace them. With respect to GPS, for instance, one could point to the fact that the beeper tracking used in *United States v. Knotts*—which the Supreme Court held was not a search—was consistent with traditional forms of surveillance in that it required an intense commitment of human and other resources,[193] whereas GPS tracking is a passive technology that eliminates the need for human agents. The Supreme Court of Washing-

[191] A third approach, taken by Chris Slobogin, is to state that the public exposure doctrine is trumped by the "reasonable expectation of privacy test," and thus set aside questions about public exposure. Slobogin, supra note 81, at 271 (arguing that "the Fourth Amendment's scope is ultimately defined by 'expectations of privacy society is prepared to recognize as reasonable,'" and that this language has superseded the "knowing exposure" language of *Katz*, calling for "an empirical inquiry into society's views about privacy"). However, Slobogin does not cite any authority that would support ignoring the public exposure doctrine.

[192] See Renee McDonald Hutchins, Tied up in *Knotts*? GPS Technology and the Fourth Amendment, 55 UCLA L. Rev. 409, 457–59 (2007).

[193] 460 U.S. 276 (1983). The Court in *Knotts* invoked this distinction: "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." Id. at 282.

ton has in fact invoked this distinction in holding that the state's constitution requires a warrant for GPS tracking: "[U]nlike binoculars or a flashlight, [a] GPS device does not merely *augment* the officers' senses, but rather provides a technological *substitute* for traditional visual tracking."[194]

Supreme Court precedents, however, offer little support for determining extrasensory status on the basis of whether technology replaces human involvement. Rather, the Court has generally made this determination on the basis of whether the information at issue could have been obtained without the technology.[195] Applying this criterion to public surveillance technologies, where the information at issue is one's visible physical location, suggests that they do not fall into the category of extrasensory technologies—as this information is arguably the same *type* of information that is gathered by traditional surveillance methods.

Unlike the information about heat sources inside a home that are detected by infrared sensors, which the Court has classified as extrasensory technology, the information about someone's location that is recorded by GPS or biometric surveillance could also be visible to the naked eye under twenty-four hour surveillance, assuming an adequate commitment of staffing and resources.[196] It is this framing of the issue that was adopted by the U.S. Court of Appeals for the Seventh Circuit prior to *Jones*, when Judge Posner concluded that the use of the GPS to track the defendant was not a search on the grounds that the Fourth Amendment "cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than they were in the eighteenth."[197] From this perspective, it seems that the difference in information gathered is merely quantitative, not qualitative—and thus not constitutionally significant. Yet this idea can be challenged with another approach.

A second way of trying to distinguish long-term surveillance technologies is to look beyond the individual pieces of information that are gathered by the technologies, to the broader picture that is produced by them. For example, as the U.S. Court of Appeals for the D.C. Circuit

[194] State v. Jackson, 76 P.3d 217, 223 (Wash. 2003) (emphasis added).

[195] See Hutchins, supra note 192, at 449.

[196] See United States v. Berry, 300 F. Supp. 2d 366, 368 (D. Md. 2004) ("A GPS merely records electronically what the police could learn if they were willing to devote the personnel necessary to tail a car around the clock."). Such around-the-clock human monitoring of one or more suspects may be practically impossible due to staffing and resource constraints, but it is hypothetically feasible.

[197] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

noted in *United States v. Maynard*, the beeper technology at issue in *Knotts* did not have the capacity for data collection or storage, and thus was limited to a discrete journey.[198] In fact, in explaining the scope of its holding, the Supreme Court in *Knotts* emphasized the importance of the "limited use which the government made of the signals from this particular beeper," explaining that as far as the record indicated the information was not used after the police followed the beeper to its location.[199] Thus, the data produced by long-term tracking technologies differ not only in terms of its quantity, but also its storage, processing, and ex post use. On the basis of this technological distinction, the D.C. Circuit concluded that the knowledge of a suspect that is produced by GPS "reveals far more than the individual movements it comprises," and thus the difference between short-term and long-term surveillance "is not one of degree but of kind."[200] The court reasoned that over a prolonged period of time, the police will learn not only facts about the person's location, but also and more importantly, facts about his or her "way of life."[201]

There are a few ways in which facts about a person's private "way of life" can be revealed through long-term tracking. First, the analysis of information about *repeated* travel can reveal one's habits, such as whether one regularly attends church, visits a particular doctor's office, or spends time in a particular type of bar. Second, the analysis of *sequences* of travel can reveal new developments in one's life; for example, "a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story."[202] Third, the analysis of the *cross-referenced* data of multiple suspects can reveal details about networks of people and associations that would otherwise remain secret. For these reasons, the D.C. Circuit concluded that what GPS tracking reveals has not been exposed, even constructively, to the public. Likewise, while Justice Sotomayor did not explicitly address the question of public exposure in her *Jones* concurrence, she expressed a similar idea in explaining why GPS tracking could implicate a reasonable expectation of privacy: "GPS monitoring generates a precise, comprehensive record of a person's pub-

[198] 615 F.3d 544, 558 (D.C. Cir. 2010).
[199] *Knotts*, 460 U.S. at 284–85.
[200] *Maynard*, 615 F.3d at 562.
[201] Id.
[202] Id.

lic movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[203] The central idea in both of the opinions is that the whole can be more than the sum of its parts.

While this "mosaic theory"[204] explanation of how the Fourth Amendment is implicated by long-term public surveillance has intuitive appeal, closer analysis reveals a problem. The problem is that the private information about someone's sexual orientation, political views, and the like, that can be gained through long-term tracking is not factual, but rather inferential. For example, with respect to sexual orientation, locational tracking can reveal that one regularly spends time at gay bars and stays the night at the house of another man, but it cannot reveal that one is gay. The facts gathered by the technology for processing and aggregation are not facts about one's sexual orientation, but rather facts about one's location, from which inferences can be made. These inferences may be either right or wrong, and the GPS data provide no way of knowing. The reason this is a problem for the mosaic theory is that the Fourth Amendment does not regulate the use of inferential reasoning by the police.[205] Rather, it regulates the collection of the underlying facts in the first instance.

It is possible that a mosaic approach could avoid this problem by stating that the mosaic that is revealed by long-term surveillance is not the personal details that can be inferred from a person's travel patterns, but rather the patterns themselves. In fact, this was the mosaic at issue in *Jones*, where the government used GPS to establish the pattern of the defendant's public movements, and then connected this pattern to information about the location of stash houses and other evidence.

However, reformulating the mosaic theory to focus on a locational mosaic—rather than a mosaic of personal information, such as political

[203] *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring). Justice Sotomayor did not explicitly address the question of public exposure, nor did Justice Alito, id. at 958 (Alito, J., concurring in the judgment), but rather they addressed this issue in the context of discussing reasonable expectations of privacy.

[204] *Maynard*, 615 F.3d at 562. While only the D.C. Circuit used the term "mosaic theory," it has since been widely used to refer to the reasoning of Justices Alito and Sotomayor. See, e.g., Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 327 (2012) (discussing Justice Alito and Justice Sotomayor's concurrences as reflecting the mosaic theory of the Fourth Amendment).

[205] See Kyllo v. United States, 533 U.S. 27, 37 n.4 (2001) ("[A]n inference is not a search.").

associations—creates a new challenge. This challenge has its origins in the mosaic theory's premise that the person under surveillance does not have a reasonable expectation of privacy in the constituent pieces of locational information that make up the mosaic. This premise is a necessary premise of the theory, as without it, the theory would not be needed.[206] Yet it also leads to a fundamental conceptual challenge highlighted by Judge Sentelle in his dissent from the D.C. Circuit's denial of rehearing en banc in *Jones*. Judge Sentelle argued that even if a whole can reveal more than the sum of its parts, this can only happen if there are parts to add into the whole, which was not the case for Jones: "The reasonable expectation of privacy as to a person's movements on the highway is . . . zero. The sum of an infinite number of zero-value parts is also zero."[207] What is needed to overcome this problem is an explanation of how all the individual pieces of locational information that are gathered by GPS have not actually been exposed to the public. This is an explanation that is to be found not in privacy, but rather in anonymity.[208]

[206] The theory is needed only when the pieces of information at issue do not, when considered independently, implicate reasonable expectations of privacy.

[207] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting from denial of rehearing en banc).

[208] Another challenge to the mosaic theory, forcefully articulated by Orin Kerr, is that it is incompatible with the "the basic structure of existing Fourth Amendment law," which Kerr argues hinges on a "sequential approach" of analysis that he describes as follows: "[T]o analyze whether government action constitutes a Fourth Amendment search or seizure, courts take a snapshot of the act and assess it in isolation." Kerr, supra note 204, at 315–16. While Kerr is right that this mode of analysis can be found in many Fourth Amendment cases, it is not essential to Fourth Amendment law and has in fact been rejected by the Supreme Court for some questions. Take, for instance, the question of whether a series of actions taken by a group of police officers in the course of an encounter with a suspect (for example, drawing a gun, physically moving the person, using handcuffs, etc.) constituted an arrest. To answer this, a court must determine whether the totality of the police officers' actions and the surrounding circumstances would have communicated to a reasonable person that he was not free to leave. See Michigan v. Chesternut, 486 U.S. 567, 573 (1988). The significance of this test is twofold: First, the series of actions can constitute an arrest even if none of the individual actions did; and second, an action taken by a police officer at the start of the encounter that did not effect an arrest at the moment it was performed (such as drawing a gun) can retroactively become part of an arrest by virtue of the subsequent actions of that or other officers (for example, physically moving the person, using handcuffs, etc.). Thus, a foundational test of Fourth Amendment law appears to reject Kerr's sequential approach of analysis and undermine his claim that the existence and duration of searches and seizures are always clear as they occur and do not turn on "ex post aggregation and analysis." Kerr, supra note 204, at 318 n.41. Further, even if Kerr's sequential approach of analysis were to be required, the mosaic theory might be compatible with it. Cf. United States v. Cuevas-Perez, 640 F.3d 272, 292 (7th Cir. 2011) (Wood, J., dissenting), cert. granted, judgment vacated, 132 S. Ct. 1534

2. Recognizing the Limits of Public Exposure

While the privacy-based framework currently employed by courts and scholars cannot adequately explain why the information captured by public surveillance technologies should not be subject to the public exposure doctrine, my analysis of the distinction between anonymity and privacy answers this question. It does so by revealing that—contrary to the assumptions of courts and scholars thus far, including advocates of the mosaic theory—not all of the individual pieces of "personal locational information" that are captured by these technologies have been exposed to the public, and for this reason, neither have the movements as a whole.

To see how this is the case, it is helpful to start with the insight developed in Part II that the secrecy of someone's personal information can be maintained by either: (1) hiding the information, or (2) hiding what makes it personal. Applied in this context, what this distinction highlights is that the secrecy of someone's "personal locational information" can be maintained if either: (1) the location of the person is hidden, or (2) the identity of the person is hidden. While these two types of information are often joined, they need not be, and thus courts applying the public exposure doctrine need to evaluate these issues separately.

For example, imagine that someone travels around the country for a month. In doing so, this person will likely expose information about the location of his body at each point along his trip, and for this reason, he will have knowingly exposed this information to the public. This is the side of the story that is highlighted by a privacy-based approach, which results in the conclusion that each piece of locational information has been exposed. There is, however, another side of the story, as the mere fact that this person has exposed the *location of his body* at each point along his trip does not mean that he will have also exposed or knowingly exposed information related to the *identification of his body* at each point. On the contrary, there may have been circumstances in which he knew or had good reason to believe that his locational information would be untraceable to his identity—that is, situations in which he had

(2012) (rejecting an ex post view of the reasonableness of surveillance, but finding that long-term GPS surveillance constituted a search on the basis of the intent of the officers at the time they attached the GPS device). Finally, while I agree with Kerr that courts addressing challenges to data aggregation will need to resolve many of the difficult questions that he has identified, see Kerr, supra note 204, at 329–30, I do not take the difficulty of these questions to speak to the issue of what is constitutionally required.

a reasonable expectation of anonymity. At these points, his *personal* locational information will not have been exposed.

Thus, courts applying the public exposure doctrine to information about a person's movements in public must inquire into whether the person had a reasonable expectation of anonymity in this information—a question for which the answer will generally depend on whether the locational information at issue in the case spans multiple places and times, or is isolated to a specific place and time.

For example, in the hypothetical of the person who travels around the country for a month, it will be difficult for this person to establish that he has not knowingly exposed his location at any point on his trip. There are two reasons for this. First, he will know that even if it is likely that he will often be anonymous during the course of his trip, the chance that he will be recognized at some point can still be non-negligible. Second, he will know that even if he is not recognized at a given time, it is likely that he will expose some distinctive features (for example, facial features, height, weight, age) that could allow for his identification retrospectively. For these reasons, he will generally not have a reasonable expectation of anonymity with respect to any given place.

However, he can nevertheless have a reasonable expectation of anonymity with respect to his trip as a whole (and this is true even if people at different points were to share information in hopes of putting together the path of his trip). The reason for this is that the probability of being recognized at consecutive points on a trip decreases exponentially with each consecutive point. For example, if the probability that the person will be recognized at any one point is 10%, the chance that he will be recognized at two consecutive points will be 1%, and the chance that he will be recognize at three consecutive points will be .1%. So as the trip becomes longer, the chance that the trip as a whole will be anonymous approaches 100%. (Note that the fact that the police might be using long-term surveillance technologies that undermine this anonymity is not relevant to the equation, as Fourth Amendment jurisprudence determines reasonable expectations according to the practices of the people one might normally encounter in public, not the specialized practices of the police.)[209] Thus, regardless of what probability of anonymity is suffi-

[209] While Orin Kerr has suggested that people cannot reasonably expect that their locational data are not being aggregated by the police because "[m]ost individuals lack a reliable way to gauge the likelihood of technological surveillance methods," Kerr, supra note 204, at 349, this argument frames the issue at the wrong level of generality. The Supreme Court

cient to constitute a "reasonable expectation of anonymity" with respect to the trip as a whole, it will be reached at some point. At this point, the fact that the given person made the trip as a whole will not have been exposed—either actually or constructively—to the public.

Furthermore, the same principle applies even if one uses a clearly identifiable form of transportation, such as a car. Although it might at first seem that someone driving a car cannot have a reasonable expectation of anonymity due to the car's uniquely identifying license plate (assuming that the car is registered to the driver), closer attention to the concept of anonymity reveals the problem with this notion. As discussed in Part II, everything that is anonymous contains some identifying information, and thus anonymity is never complete. Rather, it exists when something is known only through traits that are not, without further information or investigation, connected in a way that identifies the person in a relevant context. Applying this insight here reveals that the mere fact that a car displays a uniquely identifying trait does not mean that the driver is thereby identified. (Just as the fact that someone knows a person's name does not mean that the person is thereby identified). Rather, the driver can still be anonymous as long as someone does not connect this unique identifying trait with other identifying information, such as information in the license plate registry linking that plate number to his name, and information linking his name to his location in the relevant context. The license plate, without further inquiry, has not been connected in a way that defeats his anonymity.

Thus, a license plate is not fundamentally different from any other unique trait that might be visible on a person who is travelling by other means. It is possible that the probability of being identified *at a single point* is higher for the driver than it is for a person travelling by other means, as the license plate might make it easier to identify him. But as

does not require an inquiry into what is expected of the police specifically, but rather what is expected of others in general. For example, in *Bond v. United States*, 529 U.S. 334, 338–39 (2000), the Supreme Court addressed the question of whether a bus passenger had a reasonable expectation that his luggage would not be handled "in an exploratory manner" by a Border Patrol agent. In finding that this constituted a search, the Court explained that while "a bus passenger clearly expects that his bag may be handled[,] . . . [h]e does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner." Id. at 338–39. The relevant question was not what the passenger expected a Border Patrol agent to do, but rather what he expected other passengers or bus employees to do. If this were not the case, Fourth Amendment protections would be dictated by police practices, rather than vice versa.

with any form of transportation, the consecutive multiplication of this probability as the trip gets longer—whatever the probability of being identified at a given point along the route is—means that the chance that the trip as a whole will be anonymous will still approach 100%. When this happens, the trip as a whole will not be connected together as belonging to a single person or car, and the driver will not have exposed the fact that he made the trip.

It is important to highlight, however, that my analysis does not imply that the information gathered by *all* forms of long-term surveillance can receive Fourth Amendment protection despite the public exposure doctrine. On the contrary, an anonymity-based approach suggests that there are some forms of long-term surveillance that might not receive protection. In this way, my approach allows for the principled differentiation and fine-grained analysis that the mosaic-based approach does not.

Take, for example, the case of *United States v. Jackson*, in which the police placed a covert video camera on a telephone pole outside of the defendant's residence and recorded her comings and goings for several months.[210] While a mosaic-based approach cannot differentiate the facts of *Jackson* from those of *Jones*, as both cases involve techniques of surveillance that discover broad patterns of behavior, an anonymity-based approach reveals an important difference. The difference is that Jackson's actions all took place just outside her home—a place where the probability that one will be anonymous will generally be at its lowest. While there might be circumstances in which this is not the case, my argument here is not about whether or not Jackson lacked a reasonable expectation of anonymity on the merits, which is hard to determine from the facts as reported. Rather, my point is merely that the case illustrates how an anonymity-based approach provides criteria that are capable of differentiating between cases of long-term surveillance on normatively and legally relevant grounds, providing meaningful guidance on the question of whether the information at issue was actually or constructively exposed to the public.

While a standard based on "reasonable expectations of anonymity" will, like all standards, require difficult line-drawing at times, my analysis of the complexities of what makes something anonymous means that it is a standard that provides traction in concrete cases. For example, it reveals that things such as names and license plates do not defeat ano-

[210] 213 F.3d 1269, 1281 (10th Cir. 2000).

nymity, as nothing that is anonymous is purely so. Rather, as discussed in Part II, anonymity is a relative condition that exists in relation to a given information network, and a functional condition that exists in relation to the aims of identification.[211] Further, I have shown that anonymity should be understood as pertaining to what is known, rather than what is knowable, and thus turns on how information about a given person is connected—or aggregated—at a given moment.[212] Thus, when courts are trying to address the difficult Fourth Amendment questions posed by long-term locational surveillance technologies, an anonymity-based approach provides more concrete guidance than the mosaic-based approach developed in *Maynard* and *Jones*.

In sum, thinking in terms of anonymity rather than privacy reveals how the personal locational information gathered by long-term surveillance can, despite the public exposure doctrine, be the subject of Fourth Amendment protections. The reason is that one will at times be anonymous in public, and over time, the probability that one is anonymous at any given time will compound, making the totality of one's public movements anonymous. When this happens, this locational information is no longer publicly exposed as one's personal information. In fact, at this point, the individual locational points become disaggregated and no longer associated as points in the movement of a single person. For this reason, the mosaic approach to the Fourth Amendment concedes too much in assuming that the pieces of personal locational information that are gathered by long-term surveillance have been individually exposed—a mistake that derives from the conflation of anonymity and privacy. Thus, differentiating anonymity and privacy not only explains how the aggregation of publicly visible information can be constitutionally protected despite the public exposure doctrine, but also provides a meaningful standard—based on reasonable expectations of anonymity—that can help courts determine when aggregation implicates Fourth Amendment interests, and when it does not.

3. Protecting People, Not Places

Thinking in terms of anonymity will help courts not only identify the previously unrecognized Fourth Amendment interests that are implicated by new techniques of surveillance, but also implement the promise of

[211] See supra Section II.B.
[212] Id.

Katz that the Fourth Amendment is meant to protect "people, not places."[213] This is a promise that is thus far unrealized.

Although the Supreme Court in *Katz* moved beyond a *property*-based conception of Fourth Amendment interests, the Court has not moved beyond a *place*-based conception in the following sense: The Court finds Fourth Amendment interests when the evidence at issue is in enclosed places, such as homes, cars, packages, pockets, bags, etc., while rejecting them when it is in unenclosed places, such as the exterior of envelopes, public spaces, etc.[214] In fact, Justice Harlan's concurrence in *Katz* characterized the phone booth at issue in the case as "a temporarily private *place* whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[215]

This place-based approach does have its advantages. For example, it avoids the difficulty of basing Fourth Amendment protection on substantive judgments about what counts as a private or intimate matter, and it does "protect people" in the sense that it offers well-recognized places in which to hide secrets the assurance that they will receive Fourth Amendment protection.

However, this protection is limited by an unnecessarily constrained conception of the types of structures that can protect secrets. The only structural features of the world that the Court has recognized as protecting Fourth Amendment interests are those that protect what I have characterized as the "privacy" side of secrecy: Buildings (such as homes and offices) and shielding devices (such as envelopes, car trunks, and containers) hide facts about persons whose identities might be known. A person who uses them expects that the information contained within them will remain secret. But the structural features of our world that are

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

[214] See Kerr, supra note 204, at 316–17. Whether something is considered to be enclosed—and thus protected by the Fourth Amendment—can turn on other factors, including the location of the observer (for example, whether he is intruding on private property, or can see from a publicly accessible point), and the nature of the technology used in the observation (for example, whether it is sense-augmenting or extrasensory, and whether it is accessible to the general public).

[215] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (emphasis added). See also Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 809–10 (2004) ("[T]he basic contours of modern Fourth Amendment doctrine are largely keyed to property law. Although the phrase 'reasonable expectation of privacy' sounds mystical, in most (though not all) cases, an expectation of privacy becomes 'reasonable' only when it is backed by a right to exclude borrowed from real property law.").

capable of maintaining the secrecy of "personal information" are not limited to those that hide the *information*.

Rather, as my conceptual distinction makes clear, they can also be features that hide what makes that information *personal*—that is, features that make it anonymous.[216] Thus, in deciding whether information about a given action or set of actions is protected by the Fourth Amendment, courts should consider the structural features of the environment in which the action took place in order to determine whether the actor had a reasonable expectation of anonymity. If the action took place in physical space, relevant factors might include whether there was a crowd, whether the action took place over extended space or time, and whether any recording devices were visible. Or if the action took place online, relevant factors might include whether the actor used a pseudonym, whether that pseudonym was connected to other traits, such as an IP address, and whether that IP address was connected to the actor's name.

More generally, what recognizing this point reveals is that it is not just structural features of private life that are relevant to the Fourth Amendment, but also those features of public life. Take, for example, surveillance: Just as structural features of private life (such as the walls of one's home) can support a reasonable expectation that one's location inside will not be subject to electronic tracking by those outside, structural features of public life (such as the layout of a city, the size of the buildings, or the presence of a crowd) can support a reasonable expectation that one's location in the city over time is not being recorded. Further, just as courts evaluating the reasonableness of expectations of privacy consider proactive measures taken to protect privacy, they should likewise consider proactive measures taken to protect anonymity. For example, as Ninth Circuit Chief Judge Kozinski noted, arguing in dissent, that GPS surveillance can constitute a search: "You can preserve your anonymity from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to

[216] In this way, the relevance of the enclosed-unenclosed distinction for the Fourth Amendment (and the corresponding exclusion of unenclosed spaces from the scope of the Fourth Amendment's protection) is undermined by the recognition of the privacy-anonymity distinction (and the corresponding ways in which unenclosed information might be protected by anonymity).

be followed."[217] Focusing on the disconnectedness of traits highlights the importance of features of public space that contribute to this disconnectedness.

In addition to opening these *new types of spaces* to Fourth Amendment protection, attention to anonymity opens up new sources of *norms and laws* as the basis for those protections.[218] While property law is often cited as the quintessential enabling source of law for reasonable expectations of privacy (and the continued focus on seclusion of information is perhaps a result of this tradition),[219] reasonable expectations of anonymity are created by sources of law ranging from whistle-blowing statutes and agency law to copyright and the First Amendment, all of which grant anonymity rights.[220] In the First Amendment context, for example, the Supreme Court has held that "an author's decision to remain anonymous . . . is an aspect of . . . freedom of speech."[221] Likewise, the Court has held that the First Amendment protects a right of anonymity in one's political associations.[222]

[217] United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc). In addition, people can take various steps to compartmentalize their lives, preventing those in one social environment (for example, work) from learning about interests, beliefs, or plans we reveal to those in another environment (for example, friends).

[218] Cf. Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

[219] See Kyllo v. United States, 533 U.S. 27, 34 (2001); Minnesota v. Carter, 525 U.S. 83, 97–98 (1998) (Scalia, J., concurring).

[220] See Skopek, supra note 9, at 1759–62. Slobogin has also identified a variety of constitutional rights that are implicated by surveillance. See generally Christopher Slobogin, Privacy at Risk, supra note 191, at 98–106 (outlining the constitutional rights implicated by government surveillance). The potential to ground reasonable expectations of anonymity in law resolves one of Kerr's critiques of a mosaic theory of the Fourth Amendment, which is that "most formulations are based on a probabilistic approach to the reasonable expectation of privacy test that proves ill suited to regulate technological surveillance practices." Kerr, supra note 204, at 348. Regardless of whether the probabilistic approach is more problematic in the surveillance context than in the many contexts in which it is used by the Court (which can be questioned), the fact that this approach can be easily grounded in positive law avoids this problem.

[221] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995). This is just one of many Supreme Court cases to recognize the right. See Boudin, supra note 10, at 2165–67 (discussing the many other Supreme Court cases that have recognized an anonymity right in the First Amendment).

[222] See, e.g., Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 558 (1963) (holding that the First Amendment protected members of a political association from manda-

Further, the Supreme Court has already recognized significant substantive connections between the First Amendment's protections of speech and association and the Fourth Amendment's prohibition on unreasonable searches and seizures.[223] For example, in a series of cases the Court has held that Fourth Amendment procedures must be followed with "scrupulous exactitude" when First Amendment concerns are presented on the grounds that the "unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[224] Moreover, the Court has also implied that the First Amendment might expand or help define the scope of the Fourth Amendment's protections.[225] For example, in a case involving a sheriff who seized a copy of a film being played at a movie theater on the basis of his judgment that it was obscene, the Court held:

> The seizure is unreasonable . . . because prior restraint of the right of expression, whether by books or films, calls for a higher hurdle in the evaluation of reasonableness. The setting of the bookstore or the commercial theater, each presumptively under the protection of the First Amendment, invokes such Fourth Amendment warrant requirements because we examine what is "unreasonable" in the light of the values of freedom of expression.[226]

Thus, the Court suggested that the First Amendment implications of a search or seizure can provide a basis for a Fourth Amendment violation.

While the Court has not yet developed this idea in other cases, recognizing the role of anonymity in both the Fourth and First Amendments provides the foundation for such a development. It suggests that the scope of the Fourth Amendment's protections should be determined not

tory disclosure of their identities); Bates v. City of Little Rock, 361 U.S. 516, 523–24 (1960) (same); NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 466 (1958) (same). Other courts have applied this logic to related activities, such as reading. See, e.g., Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1053 (Colo. 2002) (holding that the First Amendment protects a right of anonymity in what one reads).

[223] The two amendments also have significant historical connections. See Daniel J. Solove, The First Amendment as Criminal Procedure, 82 N.Y.U. L. Rev. 112, 132–42 (2007).

[224] Stanford v. Texas, 379 U.S. 476, 484–85 (1965) (internal quotation marks omitted); see also United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances.").

[225] See Solove, supra note 223, at 129.

[226] Roaden v. Kentucky, 413 U.S. 496, 504 (1973); see also Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 806 (1994) (arguing that First Amendment implications should be a factor in assessing the reasonableness of a search).

only by reference to sources of law and norms that create reasonable expectations of privacy, but also by reference to the reasonable expectations of anonymity created by the First Amendment. Further, the same type of claim could be made for other sources of law that protect anonymity rights. Working out these possibilities will be the focus of another article.

The key point here is that understanding the place of anonymity in the Fourth Amendment can ground its protections in new legal and normative foundations, including a wide variety of constitutional rights and values. In doing so, it can provide a foundation for Justice Sotomayor's suggestion in *Jones* that when applying the Fourth Amendment to cases of long-term surveillance, she would "ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on."[227]

Finally, thinking in terms of anonymity reveals new ways of mitigating the Fourth Amendment concerns posed by new surveillance technologies. When the Fourth Amendment is conceptualized in terms of privacy, strategies that *seclude* our personal information appear to be the only solution; whereas when seen in terms of anonymity, it becomes clear that we can also look for strategies that *disaggregate* our information. For example, the extent to which video camera surveillance implicates anonymity turns in part on whether the video data are generally reviewed by someone, archived for future use, analyzed for patterns, indexed according to who and what is shown, and cross-referenced with other surveillance data. Thus, by limiting it across any one of these dimensions, the invasion of anonymity can be limited. By drawing our attention to these potential points of disaggregation, an anonymity-based approach can help us design surveillance strategies that do not implicate the Fourth Amendment.

In sum, there are three core ways in which thinking in terms of anonymity can help courts fulfill the promise of *Katz*. First, this approach reveals that the structures that protect Fourth Amendment interests are not just the buildings and containers that hide our information, but also the features of public space that hide what makes our information personal. Second, this approach opens up new enabling sources of law for Fourth Amendments interests, including the First Amendment and other

[227] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

protections of individual liberties. Third, it points to ways in which surveillance can be tailored to avoid implicating these interests while still being an effective police tool.

CONCLUSION

The Supreme Court has concluded that the Fourth Amendment's protections do not apply to information that has been exposed to the public or third parties. Privacy scholars have argued that this reasoning is flawed on the grounds that privacy is not a binary condition, but rather something that exists in degrees. While this critique is correct as far as it goes, it only identifies part of the problem. What it fails to recognize is that the public exposure and third party doctrines also derive from a mistaken conflation of anonymity and privacy. Although anonymity and privacy are similar in that both maintain the secrecy of personal information, they differ in a fundamental and legally relevant way: Privacy hides the information, whereas anonymity hides what makes it personal. Understanding this difference reveals the reasons why and ways in which the Fourth Amendment should be interpreted to protect not only reasonable expectations of privacy, but also "reasonable expectations of anonymity."

In addition to revealing why the Fourth Amendment should protect anonymity interests as a general matter, this Article provides the analytic tools needed to answer difficult and pressing questions about specific new techniques of data collection and analysis. For example, it provides courts with a principled standard that not only identifies otherwise-unrecognizable ways in which new surveillance practices implicate the Fourth Amendment, but also differentiates seemingly similar practices that do not. Furthermore, at a more fundamental level, it helps courts apply the Fourth Amendment in ways that bring us closer to the promise in the Supreme Court's canonical statement that "the Fourth Amendment protects people, not places."[228]

Finally, while this Article has focused on surveillance and the Fourth Amendment, its insights are applicable to other practices and sources of law that protect reasonable expectations of privacy.[229] Take, for exam-

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

[229] These include tort law, the Freedom of Information Act, the Privacy Act of 1974, the constitutional right of information privacy, and various evidentiary privileges. Strahilevitz, supra note 96, at 985–86. Wherever these sources of law adopt a purely descriptive concep-

ple, the legal interests at stake in activities ranging from dialing phone numbers and making purchases online, to donating blood or having tissue removed. While these interests have previously been analyzed under the framework of privacy, this approach may often be misguided. The reason is that when we engage in these activities, we do not always expect that the *information* contained in our phone logs, purchases, blood, and tissue will remain unknown. Rather, what we often expect to remain unknown is the fact that this information is information *about us*. We expect that when a company connects our phone calls and processes our online orders, and when doctors bank our blood or dispose of our tissue, these things become part of an undifferentiated flow—that they become anonymous. Thus, for our law to adequately respond to the emergence of big data practices that collect, store, and aggregate these types of information, we need to be thinking in terms of anonymity as well as privacy. It is only in this way that we will be able to recognize and protect the important legal interests that are implicated by these new threats to the secrecy of our personal information.

tion of "reasonable expectations of privacy," they should also—on both substantive and formal grounds—protect "reasonable expectations of anonymity." This is, at the very least, true of tort law. See id. at 932–35 (identifying the ways in which, and reasons why, courts adopt a non-normative and non-content based conception of the "reasonable expectations of privacy" element of privacy torts). When this is not the case, the lessons of this Article will not be outcome-determinative in this way, though they will still have significant relevance.