CONTEXTUAL EXPECTATIONS OF PRIVACY

Andrew D. Selbst†

Fourth Amendment search jurisprudence is nominally based on a "reasonable expectation of privacy," but actual doctrine is disconnected from society's conception of privacy. Courts rely on various binary distinctions: Is a piece of information secret or not? Was the observed conduct inside or outside? While often convenient, none of these binary distinctions can adequately capture the complicated range of ideas encompassed by "privacy." Privacy theorists have begun to understand that a consideration of social context is essential to a full understanding of privacy. Helen Nissenbaum's theory of contextual integrity, which characterizes a right to privacy as the preservation of expected information flows within a given social context, is one such theory. Grounded, as it is, in context-based normative expectations, the theory describes privacy violations as unexpected information flows within a context, and does a good job of explaining how people actually experience privacy.

This Article reexamines the meaning of the Fourth Amendment's "reasonable expectation of privacy" using the theory of contextual integrity. Consider United States v. Miller*, in which the police gained access to banking records without a warrant. The theory of contextual integrity shows that* Miller *was wrongly decided because diverting information meant purely for banking purposes to the police altered an information flow in a normatively inferior way. Courts also often demonstrate contextual thinking below the surface, but get confused because the binaries prevalent in the doctrine hide important distinctions. For example, application of the binary third-party doctrine in cases subsequent to* Miller *obscures*

† J.D. 2011, University of Michigan Law School; M.Eng. 2005, S.B. 2004, Massachusetts Institute of Technology. Alan Morrison Supreme Court Assistance Project Fellow, Public Citizen, Washington D.C. Thanks to the faculty and 2011-12 fellows of the Information Law Institute—Roger Ford, Joe Hall, Helen Nissenbaum, Ira Rubenstein, and Kathy Strandburg for helping me think through contextual integrity and the Fourth Amendment. Thanks also to Bryan Choi, Catherine Crump, Michael Froomkin, James Grimmelmann, Ian Kerr, Orin Kerr, Erin Murphy, Eve Brensike Primus, Chris Slobogin, Ben Wizner, Felix Wu, the members of the Privacy Research Group, attendees of the 2012 Privacy Law Scholars Conference, for helpful discussions and comments. This Article reflects my personal views only and was not written pursuant to my role at Public Citizen. This research was supported by the following grants: Air Force Office of Scientific Research: ONR BAA 07-03 (MURI) and NSF CT-M: Privacy, Compliance, & Information Risk CNS-0831124.

important differences between banking and other settings. In two recent cases, United States v. Jones *and* Florida v. Jardines*, the Supreme Court has seemed willing to consider new approaches to search, but they lacked a framework in which to discuss complicated privacy issues that defy binary description. In advocating a context-based search doctrine, this Article provides such a framework, while realigning a "reasonable expectation of privacy" with its meaning in society.*

TABLE OF CONTENTS

INTRODUCTION

In the last two years, the Supreme Court has issued two decisions that augur a fundamental change in the nation's approach to the Fourth Amendment. In January 2012, the Supreme Court unanimously decided

in *United States v. Jones*[1] that using a Global-Positioning System (GPS) device to track a suspect for a month is a "search" under the Fourth Amendment.[2] The Court issued three opinions, however, disagreeing over the legal rationale to support that conclusion.[3] On the one hand, the majority opinion held that the GPS tracking at issue was a search because the police trespassed against the property of the defendant.[4] This reasoning contradicted forty-five years of settled precedent that understood a "reasonable expectation of privacy" (the *Katz* test) as the touchstone in determining whether a "search" occurred and that the Fourth Amendment protects "people, not places."[5] On the other hand, a total of five concurring Justices agreed that at the least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy,"[6] but they were unable to articulate a theory as to why.[7]

In March 2013, the Court decided in *Florida v. Jardines*[8] that when police use a trained dog to sniff for drugs at a person's home, it implicates the Fourth Amendment.[9] Again the opinions split between the majority's trespass-based holding and a concurring opinion's privacy-based rationale. Both opinions refer to the importance of social context, and as in *Jones*, the privacy-based opinion contradicts long-held assumptions regarding how the Court reasons about "reasonable expectations of privacy."[10]

Both cases illustrate the difficulties with search doctrine's reliance on binary distinctions, such as whether a piece of information is "private" or "public." In *Jones*, the search occurred in "public," outdoors, and yet all nine Justices intuited that the Fourth Amendment had been implicated.[11] Because the doctrine relied on a public/private distinction,[12] none of the Justices could convincingly describe why the use of GPS was a search within the language of the doctrine. In *Jardines*,

---

1 132 S. Ct. 945 (2012).

2 *Id.*

3 *Id.*

4 *Id.* at 949.

5 Katz v. United States, 389 U.S. 347, 351, 360 (1967).

6 *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (internal quotation marks omitted); *id.* at 964 (Alito, J., concurring).

7 *See, e.g.*, Tom Goldstein, *Why* Jones *Is Still Less of a Pro-Privacy Decision than Most Thought (Conclusion Slightly Revised Jan. 31)*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought ("Beyond that, what are the details of the Alito theory and what does it mean? Many initially read the Alito concurrence as a strong statement favoring individual privacy in a modern age. I think that is very wrong. The opinion openly struggles with these issues.").

8 133 S. Ct. 1409 (2013).

9 *Id.*

10 See discussion of Justice Kagan's *Jardines* concurrence *infra* Part IV.

11 *Jones*, 132 S. Ct. at 949.

12 *See id.* at 950.

Justice Kagan's concurrence recognized that both a dog sniff and powerful binoculars peering into the home could invade privacy.[13] According to prior doctrine, however, the open window likely meant that a person had no reasonable expectation of privacy, and binoculars would not have triggered a Fourth Amendment search.[14]

Though two majority holdings have now adopted the trespass rationale, *Katz*'s privacy-based rationale remains central to search doctrine. As the concurring Justices explained in *Jones*, a physical trespass rule is not enough protection[15] because the surveillance technologies being deployed today—cell site monitoring, drones, automatic license plate recognition, surveillance cameras, and social networks—do not need physical access to work.[16] Doctrinally, the cases both stressed that the trespass test supplements rather than supplants the *Katz* test, and thus the *Katz* test lives on.[17]

The *Katz* test has long been criticized. To be tied to society's reasonable expectations of privacy, the law must meaningfully engage people's actual experience of privacy. Currently, the Fourth Amendment lacks such a foundation. This is not entirely surprising, however, as understanding the nature of privacy has proven a monumentally difficult task.[18] Various formulations have been proposed over the years, including Warren and Brandeis's famous "right to be let alone,"[19] the right to secrecy,[20] control over personal information,[21] a right to intimacy,[22] and a right to personal autonomy.[23]

---

13 *Jardines*, 133 S. Ct. at 1418 (Kagan, J., concurring).

14 *See* Minnesota v. Carter, 525 U.S. 83, 104 (1998) (Breyer, J., concurring) (comparing an open window to *Florida v. Riley*, 488 U.S. 445, 448 (1989) (finding observation of greenhouse from helicopters in public airspace permissible, even though owners had enclosed greenhouse on two sides, relied on bushes blocking ground-level observations through remaining two sides, and covered 90% of roof) and *California v. Ciraolo*, 476 U.S. 207, 209 (1986) (finding observation of backyard from plane in public airspace permissible despite six foot outer fence and ten foot inner fence around backyard)).

15 *Jones*, 132 S. Ct. at 963.

16 *See infra* Part IV.

17 *Jardines*, 133 S. Ct. at 1417 ("The *Katz* reasonable-expectations test 'has been *added to,* not *substituted for,*' the traditional property-based understanding of the Fourth Amendment." (quoting *Jones*, 132 S. Ct. at 952)); *Jones*, 132 S. Ct. at 953 ("[U]nlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test."); *id.* at 954–55 (Sotomayor, J., concurring) ("I join the Court's opinion because I agree that a search . . . occurs, at a minimum, '[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area.' . . . Of course . . . . even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" (alteration in original) (citations omitted)).

18 Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1088, 1088–89 (2002).

19 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

20 Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 405 (1981).

21 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Solove, *supra* note 18, at 1108–09.

22 JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 74 (1992).

23 Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992).

Legal formulations in particular tend to focus on binary distinctions, presumably because they provide relatively easy lines for law enforcement officials and judges to draw. Specific definitions of "private" and "public," however, differ depending on who is asked, and in what context.[24] Some definitions rely on whether information is secret or not, whether conduct occurs inside or outside, or whether the kind of conduct is in some general sense normatively private/intimate or not.[25] The one similarity between all these definitions is the reason they all fall short: they are all binaries.[26]

Each of these binaries has proven inadequate, unable to capture society's definition of "privacy." In public view, stalking someone is still a privacy violation.[27] In social relationships, people often share information with others that they wish to be kept private from the world at large. In fact, the degree of sharing is one of the primary factors defining social relationships.[28] This information is neither secret nor "public."

Technology accentuates the binaries' deficiencies. Are shopping habits private or public? On the Internet, consumers are constantly tracked, often leading to useful recommendations at Netflix and Amazon, but most people would call security after being followed around a mall for two hours.[29] Court records and gun ownership records are presumptively public, but there is a difference between having to go to the courthouse or county records office to dig through files and a simple no-cost web search open to potential employers, insurance companies, and romantic interests.[30] Social media have enhanced people's ability to share photos and amusing or embarrassing stories, and many have embraced this new technological capacity. As a result, many who are used to thinking of privacy in binary terms erroneously claim that young people just do not care about privacy, when in reality, they merely conceive of it differently.[31]

---

24 HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 89–98 (2010).

25 *Id.* at 90.

26 *See id.*

27 *See, e.g.*, 720 ILL. COMP. STAT. 5/12-7.3(a-3) (2013); MICH PENAL CODE § 750.411h; N.Y. PENAL LAW § 120.45 (McKinney 2013).

28 Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 924 n.9 (2005); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 521 (2006).

29 *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998).

30 Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma, *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772 (2012); J. David Goodman, *Newspaper That Put Gun Permit Map Online Hires Armed Guards*, N.Y. TIMES, Jan. 3, 2013, at A19.

31 CHRIS HOOFNAGLE ET AL., HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES & POLICIES? (2010).

The problem with binaries is that to employ them is to attempt the impossible—to simplify privacy by abstracting away the context. Recent privacy law scholarship has focused a great deal on privacy theories derived from social context.[32] Robert Post recognized that the public disclosure tort's reliance on the "reasonable person['s]" sense of what is "highly offensive" bases privacy judgments on social contexts.[33] Daniel Solove set out in 2002 to "suggest an approach to conceptualize privacy from the bottom up rather than the top down, from particular contexts rather than in the abstract."[34] Orin Kerr has argued that the Supreme Court has unwittingly used context-dependent theories of the Fourth Amendment,[35] and then argued that doing so makes perfect sense because nothing else will work.[36] Lior Strahilevitz argued for a theory of privacy based on the practical likelihood of information dissemination given what we know about social networks.[37] Katherine Strandburg has argued that privacy law should be sensitive to the "exploding variety of contexts" on the Internet.[38]

All this scholarship stresses the importance of social context as well as recognizing the impossibility of a privacy definition that excludes it. In Helen Nissenbaum's theory of contextual integrity, however, privacy is not just related to context, but is instead defined as adherence to the norms of information flow specific to that context.[39] As she wrote in *Privacy in Context*, her book presenting the theory:

> [A] right to privacy is neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information. . . . Privacy may still be posited as an important human right or value worth protecting through law and other means, but what this amounts to is a right to contextual integrity and what *this* amounts to varies from context to context.[40]

---

32 *See, e.g.*, Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 507 (2007); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957 (1989); Solove, *supra* note 18, at 1092–93; Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619–21 (2011).

33 Post, *supra* note 32, at 962.

34 Solove, *supra* note 18, at 1092.

35 Kerr, *supra* note 32, at 507.

36 *Id.* at 525.

37 Strahilevitz, *supra* note 28, at 921 ("[P]rivacy tort law should not focus on the abstract, circular, and highly indeterminate question of whether a plaintiff reasonably expected that information about himself would remain 'private' after he shared it with one or more persons. Instead, the law should focus on the more objective and satisfying question of what extent of dissemination the plaintiff should have expected to follow his disclosure of that information to others.").

38 Strandburg, *supra* note 32, at 619.

39 NISSENBAUM, *supra* note 24.

40 *Id.* at 127.

Drawing on Professor Nissenbaum's theory of contextual integrity, this Article posits a context-based Fourth Amendment search doctrine, creatively dubbed "contextual search." With its focus on context, Professor Nissenbaum's theory can give the "reasonable expectation of privacy" test the grounding it currently lacks. The main contribution of the theory is its descriptive power; it does an excellent job explaining how people in society actually experience privacy. Additionally, while contextual integrity cannot, by itself, answer many of the resulting normative questions that arise in its application, it can also provide constraints and structure to judicial decision-making that do not exist in current understanding of search doctrine.

This Article is divided into five Parts. Part I introduces the theory of contextual integrity. The theory has both descriptive and normative components. The descriptive component fleshes out the meaning of "reasonable expectation of privacy" in a context-conscious society. The normative component treats disruptive information flows as prima facie violations of contextual integrity and considers whether the disruptive flow might be superior to entrenched flows for one reason or another.

Part II offers an overview of the current search doctrine under the *Katz* test. It also introduces some common critiques of the doctrine and examines how some of these critiques are addressed by contextual search. Part III puts the theory into practice, examining several different areas of Fourth Amendment search doctrine and the canonical cases that accompany them. It discusses how the cases could have turned out differently if analyzed under contextual search, with an eye toward illustrating the general structure of such analysis.

Where Part III examines past cases, Part IV looks to the future of the Fourth Amendment, anticipating the increasing prominence of emerging technologies in future cases. This Part discusses how technology cuts across different contexts, reducing costs for information flow and storage, thus causing previously unforeseen disruptions in information flows. It then examines a few such technologies and their accompanying information flows.

Part V steps outside of search doctrine to find areas in current Fourth Amendment jurisprudence where context is implicitly recognized. The discussion demonstrates that a context-conscious doctrine would have the added benefit of pulling together previously disjoint pieces of current doctrine under a more unified theory. Finally, this Article concludes that implementation of contextual search would unsettle the doctrine, but the benefits of doing so likely outweigh the uncertainty created. *Jones* and *Jardines* seem to signal the Court's willingness to embrace a new approach, perhaps even one based on social context. This Article proposes one such approach.

I. INTRODUCTION TO CONTEXTUAL INTEGRITY

Contextual integrity is a theory describing how contemporary liberal societies view privacy on the ground. It contends that consensus about defining public and private, or the line between them, has been difficult to reach because there is no single line and there is no single concept of private and public. According to the theory, society's implicit understanding of privacy is respect for the *appropriate* flow of information about identifiable persons within particular social contexts.[41] The theory has a descriptive layer and a normative layer. The descriptive layer identifies when contextual integrity is achieved or violated, and the normative layer evaluates whether the new information flows being tested are preferable to the status quo.

The principle of appropriateness is different from the principles of secrecy or control, recognizing that in many circumstances the sharing of information is itself beneficial and an account of privacy should differentiate between beneficial and harmful sharing. Appropriateness is expressed in the construct of a "context-relative informational norm[]," a subspecies of social norm that governs how information is expected to flow among social actors within a given social context.[42] People's indignation, anxiety, fear, anger, and outrage over a privacy violation are evidence that an informational norm has been breached, and protest and resistance often follow. Contextual integrity is achieved when informational norms are respected.

Contextual integrity relies on the background assumption that social contexts are an organizing principle of social life.[43] Accordingly, people "act and transact not simply as individuals in an undifferentiated social world," but as actors "in certain capacities . . . in . . . a plurality of distinct social contexts."[44] These "[c]ontexts are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)."[45] Familiar contexts include healthcare, the marketplace, finance, politics, religion, education, friends, and home life.[46] Each of these contexts has its own set of informational norms that govern the relationship between actors and information.

---

41 *Id.* Information flow is comprised of sharing, capture, disclosure, communication, and dissemination of information. *Id.*

42 *Id.* at 129.

43 As a general proposition, this is a widely accepted position of established social theory. The particulars of *how* social contexts structure social life vary between different theories. Contextual integrity is agnostic as to these particulars. *Id.* at 129–32.

44 *Id.* at 129–30.

45 *Id.* at 132.

46 *Id.* at 130.

As defined in the theory, there are three component parts to an informational norm: actors, attributes, and transmission principles. Actors are the people or institutions involved. They can be the *subjects*, *senders*, or *receivers* of the information. Attributes are what the information is about—whether it is a health record, name of an associate, a location, or a piece of gossip, for example. Transmission principles are restrictions placed upon the flow of information between the actors by the particular context: the "rule" part of the norm. Common transmission principles include *control* over information or *withholding* information, but those are merely two of an infinite range of possibilities, including, for example, information *shared in confidence*, *obtained with authorization*, *obtained under compulsion*, *held in fiduciary care*, *sent for a specific limited purpose*, or *obtained with a warrant*.[47]

The construct of an informational norm distinguishes contextual integrity from other accounts of privacy in that all the variables—actors, attributes, and transmission principles—and implicitly, the contexts from which they are derived, matter simultaneously. Thus, an informational norm can be as straightforward as the rule that a priest must hold a confessed sin in confidence or as complex as the expectation that each of the pieces of information provided to the Internal Revenue Service in an annual tax return will be sent only to the appropriate parties as described by law. Additionally, because informational norms are derived from their social context, their structures vary widely. Informational norms, much like law itself, can fluctuate between fully specified rules and basic principles. The sources of norms can be law, professional codes, or merely ideas implicitly woven into "the very fabric of social and political life."[48]

The concept is best illustrated with an example. In the healthcare context, a patient will often share information with a doctor for the purpose of obtaining medical care. The doctor will then share information with other members of her staff—hospital administrators, other doctors, or nurses. When the doctor shares information with a nurse, the doctor is the *sender*, sharing information with the nurse as the *receiver*, about the patient as the *subject*. The attribute in this case is medical information (unless it is insurance information, which will have its own rules) and the transmission principle is something approximating *open sharing of medical information within the hospital for the purposes of medical evaluation, and confidentiality with respect to all others except immediate family*. As applied to medical personnel, then, open sharing is the rule. If the doctor shared medical information with the patient's employer, however, that would violate the

47 *Id.* at 145.
48 *Id.* at 128.

informational norm because the rule regarding all non-immediate family or hospital staff is *confidentiality*. A violation cannot be determined without reference to all the parts: the actors, attribute, and transmission principle. Note also the difference between this and a control-based information regime. Patients do not always expect the doctor to seek approval before transmitting information to other medical professionals. They instead expect the norm to be respected.

In terms of analytical procedure, the descriptive layer can be broken down further into two parts: the "framework analysis" and the "violation inquiry."[49] The framework analysis identifies the relevant informational norms. Once the framework is established, the analysis of the actual information flows (e.g., who heard what piece of information) is the violation inquiry. This inquiry determines whether the norms identified in the framework analysis were *actually* violated. If the norms were violated, then that is a prima facie violation of contextual integrity.[50] That is the descriptive layer.

The normative layer attempts to provide a method of distinguishing between advances in law or technology that could be seen as beneficial in the balance and those advances that are harmful by borrowing extrinsic moral and political value judgments, but constraining them to be sensitive to context. The normative layer compares entrenched and disruptive flows in two ways. The first assesses the general moral and political impacts of the changed flow, asking what and whose interests are affected, whether and what harm is caused, and what political or moral values are affected. Widening power imbalance, diminishment of liberty, autonomy, equality, efficiency, justice, or security, and escalation of prejudice or unfair discrimination are all effects to consider.[51] The second evaluation is context-specific and is the theory's main contribution in the normative debate. It asks whether a new flow better serves the values or purposes of the relevant social context.

The importance of this second evaluation is most clearly demonstrated in the case of disruptions that threaten the integrity of the context itself. For example, in the healthcare context, the increasing prevalence of electronic medical records radically disrupts information flows. When evaluating such records, full consideration must be given, not only to harms and benefits to patients and other medical actors, but also to how these new flows affect the achievement of health and the alleviation of physical suffering irrespective of social status or wealth; all

---

49 Professor Nissenbaum does not herself break descriptive layer into parts; I have found that it makes the analysis clearer to do so, and it does not change the operation of the theory.

50 The two parts are analogous to the "law" and the "facts" of the descriptive layer.

51 There is a large body of work discussing the value of privacy to both the individual and society. For a short summary of it and sources, see NISSENBAUM, *supra* note 24, at 74–88.

of which are foundational values of the healthcare context. If changes in information flows, such as the sale or theft of medical information that is now electronically recorded, lead patients to avoid tests or to lie to physicians, then these ends and values are undercut and the new flows cannot be supported. As another example, when considering whether a police officer may search a student's locker, it is important to consider the intrusive effect of police on school systems and whether a teacher's ability to search lockers might accomplish the same law enforcement goals with less disruption.[52] These normative concerns recognize that the contexts themselves are foundational to society, and it is important to allow them to thrive.

One significant and quite difficult question in applying contextual integrity is the appropriate choice of context. Some contexts exist as subsets of others: Is the smaller "law enforcement" context or the more general "political" context more salient? How about "markets" or "markets for highly regulated items?" Many situations involve overlapping contexts as well. When a hospital reports a shooting, as it is often required to do by law,[53] do the norms of the healthcare or law enforcement context control? The context must be identified at the beginning of the analysis, yet the choice of context is itself a normative question because it defines the values and thus the informational norms at stake.[54] Accordingly, arguments about the relevant value considerations often appear as arguments about the most salient context.

Michael Birnhack, reviewing Professor Nissenbaum's book, described this as a major flaw of contextual integrity.[55] Rather than being a fatal flaw of the theory, however, this unavoidable reality merely makes the decision about choice of context iterative. If one considers a few of the most plausible contexts in a parallel manner, different rules emerge in each. Executing the analysis demonstrates how the choice of context affects the outcome.[56] After analyzing the different possible choices in parallel, the resolution of a classic normative debate will point to which choice of context was "correct." In many cases, this iterative process is not necessary because the context is fairly well understood, but unsurprisingly, borderline cases are going to be hard to analyze, and

---

52 *See* New Jersey v. T.L.O., 469 U.S. 325, 349–50 (1985) (Powell, J., concurring).

53 Debra Houry et al., *Violence-Inflicted Injuries: Reporting Laws in the Fifty States*, 39 ANNALS OF EMERGENCY MED. 56 (2002); *see, e.g.*, IND. CODE ANN. § 35-47-7-1 (West 2013); LA. REV. STAT. ANN. § 14:403.5 (2013); N.Y. PENAL LAW § 265.25 (McKinney 2013).

54 Michael D. Birnhack, *A Quest for a Theory of Privacy: Context and Control*, 51 JURIMETRICS J. 447, 469 (2011) (reviewing NISSENBAUM, *supra* note 24) ("[D]efining a context becomes a process subject to the interpretation of the observer (or perhaps manipulation by an interested party).").

55 *Id.*

56 See *infra* note 219 for an example.

contextual integrity's application in the law will ultimately have to be resolved by judge or jury (common law being its own form of iteration).[57]

The normative layer effectuates a form of stare decisis within contextual integrity itself. Contextual integrity contains a presumption in favor of precedent, though it is not quite as strict a presumption as stare decisis in law.[58] If and only if a new practice is normatively preferred after being compared with the old, that practice is incorporated into the framework of that context for the future as an amendment to the transmission principle going forward. If, for example, the normative layer determines that society believes that police should hear about bullet wounds, then the healthcare transmission principle will be modified to permit information about bullet wounds flowing to police. Thus, once a normative ruling is made, it functions as the new default rule.

The reverse is also true. If there is no violation, the theory must determine that the context is not too permissive. This symmetry is important so that contextual integrity can determine that an entrenched practice is flawed, based either on the argument that it was flawed to begin with, or that circumstances and attitudes have changed such that an established practice is now offensive to norms. As a result of this stare decisis element, contextual integrity functions well as a theoretical foundation for a common law doctrine.

II. THE *KATZ* PARADIGM AND ITS PROBLEMS

The Fourth Amendment to the Constitution reads, in part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[59] Courts employ a two-part test to determine whether there was a Fourth Amendment violation due to a search: 1) Was the police action in question a "search?" and, if so, 2) was the search reasonable?[60] If a court finds that the action was not a search, then the Fourth Amendment simply does not apply, and the query has ended.[61] If the action was legally a search, then the doctrine requires that the

---

57 If the relevant inquiry is a "reasonable expectation"—an inherently social question—then I do not see why the result could not be an issue of fact for the jury, rather than a question of law for the judge.

58 *See* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 854–55 (1992) (discussing stare decisis as a strong presumption, but not quite an "inexorable command").

59 U.S. CONST. amend. IV.

60 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 32 (2011).

61 *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31–32 (2001) (describing the question of "when a search is not a search" is antecedent to the question of reasonableness).

search be justified by either a warrant or a recognized exception to the warrant requirement, coupled with the appropriate level of suspicion (e.g., probable cause or reasonable, articulable, particularized suspicion). If the police had no warrant and no applicable warrant exception, then the search was not reasonable and a Fourth Amendment violation has occurred.

Since *Katz v. United States*,[62] "search" has been defined as an action by a government actor that violates a "reasonable expectation of privacy"[63] (or, after *Jones* and *Jardines*, involves a trespass).[64] The definition of "reasonable expectation of privacy," however, is unclear and inconsistent across different legal and social contexts. Various scholars have called the current state of the doctrine an "embarrassment,"[65] "unstable,"[66] and "a series of inconsistent and bizarre results that [the Supreme Court] has left entirely undefended."[67]

Search doctrine is completely disconnected from society's actual expectations of privacy. For example, if a person is outdoors, in public, he generally has no reasonable expectation of privacy, even if he expects that he is alone and unwatched.[68] The Supreme Court's approach to this concept has been unforgiving, treating any risk at all of exposure as de facto exposure.[69] For example, in both *California v. Ciraolo*[70] and *Florida v. Riley*,[71] the Court ruled that because someone could *theoretically* rent a plane and fly over property, it was unreasonable to expect that the activities on the property were hidden despite measures clearly taken to hide them, such as high fences.[72]

Similarly, if a piece of information is accessible to anyone other than a government official, the act of retrieving it is outside the purview

62 389 U.S. 347 (1967).

63 *Id.* at 360 (Harlan, J., concurring).

64 After *United States v. Jones*, the search inquiry also asks whether there was a trespass, but here I am only concerned with the *Katz* test, which operates as a separate, but parallel test for finding a violation. United States v. Jones, 132 S. Ct. 945, 952 (2012) ("[A]s we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

65 Kerr, *supra* note 32, at 505; *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757 (1994).

66 Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

67 Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 29 (1988).

68 *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1010 (2010).

69 Colb, *supra* note 66, at 121–22.

70 476 U.S. 207 (1986).

71 488 U.S. 445 (1989).

72 *Id.* at 448; *Ciraolo*, 476 U.S. at 210.

of the Fourth Amendment.[73] This is true of records kept by banks[74] and lists of phone numbers that a person calls.[75] It also likely applies to information collected by private companies on the Internet, such as Amazon, Google, Facebook, and Twitter (which collect location data, search habits, and purchase histories),[76] not to mention *posts* to social networks, irrespective of the chosen privacy setting.[77] Undoubtedly, at least some of this information would be reasonably considered private by most of society.[78]

Many of these curious results can be traced back to four conceptual problems in the development of search doctrine. First, the doctrine has too often focused on binary distinctions, such as whether a person is inside or outside.[79] This problem is illustrated by the concurring Justices' difficulty explaining their collective intuition in *Jones*: that despite Antoine Jones's car being outdoors, constantly tracking it for a month with no warrant was a violation of the Fourth Amendment.[80] Second, the *Katz* doctrine has often been criticized as "unstable"[81] or "circular."[82] Stemming from Justice Harlan's concurrence in *Katz*, the current "reasonable expectation of privacy" test has objective and subjective halves.[83] These halves, roughly speaking, equate to 1) whether society would recognize a privacy interest, and 2) whether a person individually seeks to protect that interest.[84] The two halves are often conflated in current law, resulting in the following tautology: Once a privacy violation is known, it is unreasonable for a person to expect that

---

73 United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . .").

74 *Id.*

75 Smith v. Maryland, 442 U.S. 735 (1979).

76 *E.g.*, Somini Sengupta, *Law Enforcement Rarely Uses Search Warrants in Getting Twitter Data*, N.Y. TIMES BITS BLOG (Jan. 28, 2013, 5:00 PM), http://bits.blogs.nytimes.com/2013/01/28/law-enforcement-rarely-uses-search-warrants-in-getting-twitter-data.

77 E-mail and text messages, at least, seem likely to be protected. Strandburg, *supra* note 32, at 642.

78 *See, e.g.*, JAN LAUREN BOYLES, AARON SMITH & MARY MADDEN, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES 2 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf ("More than half of app users have uninstalled or decided to not install an app due to concerns about personal information. . . . Cell phone owners take a number of steps to protect access to their personal information and mobile data.").

79 Kerr, *supra* note 68, at 1010 ("The distinction between government surveillance outside and government surveillance inside is probably the foundational distinction in Fourth Amendment law . . . .").

80 United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 958 (Alito, J., concurring).

81 Colb, *supra* note 66, at 122.

82 Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106 (2008); *see also* Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188.

83 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

84 *See infra* Part III.B.

his privacy is intact, and therefore, there is no reasonable expectation of privacy. This formulation, if accepted, would eviscerate the Fourth Amendment. Third, the Fourth Amendment's distortion of the word "search" has exempted certain categories of police tactics, such as following a person indefinitely or digging through his trash,[85] from Fourth Amendment consideration without any attempted justification. If society's privacy expectations are supposed to be the driving force behind the doctrine, it is important that the terms used correspond to common English language usage. Fourth, courts often make normative judgments about whether one rule or another is preferable, regarding the permissibility of a particular kind of police action. These judgments pit officer certainty and bright line rules against a more nuanced approach and hazily defined privacy rights. Due to the conceptual failures above and the incoherence of the doctrine, courts lack meaningful guidance in making these evaluations.

These problems are not an inevitable byproduct of *Katz* or a privacy-focused regime.[86] All four can be addressed by contextual search. Contextual search eschews binary definitions of privacy, instead recognizing that privacy expectations cannot be extracted from their social context. The analytical structure of the theory replaces the objective and subjective elements with the framework analysis and violation inquiry, which cannot be conflated as the word "expectation" can in its dual deployment. At the same time, the word "search" is restored to its original meaning in the English language, and the descriptive Fourth Amendment inquiry is reduced to a single step: whether a given search was reasonable. Finally, the normative analysis provides a structure for judicial decision-making, in that it instructs courts to consider the values of the social context in addition to the general Fourth Amendment concerns.

A. *Binaries and Confusion About Context*

The binary structure of the current doctrine is the first major conceptual flaw. Current Fourth Amendment doctrine considers too few facts while attempting to answer whether there is a reasonable expectation of privacy. If the only relevant consideration is whether a person is inside or outside, or information is secret or not secret, judicial

85 California v. Greenwood, 486 U.S. 35, 41 (1988).

86 *Contra* Christian M. Halliburton, *How Privacy Killed* Katz*: A Tale of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm*, 42 AKRON L. REV. 803, 810–11 (2009); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1758–63 (1994).

and policing decisions are easier, but these binaries cannot capture society's expectations of privacy.

Before *Jones*, many assumed that people have no reasonable expectation of privacy when outdoors.[87] In reality, however, whether a person is indoors or outdoors is not enough information to determine if there is a privacy breach. Stalking is a well-recognized privacy violation that can occur entirely outdoors. The same is true of paparazzi taking salacious photographs.[88] No one thinks the police can pull down someone's pants for evidence just because they are on the street.[89] These cases contradict the notion that there is no privacy in public. The public/private distinction fails even *within* current doctrine.

The binary structure also fails for information sharing. The third-party doctrine treats information shared with one person as shared with the world.[90] The doctrine cannot handle the concept of sharing a secret with one or two friends and experiencing a privacy breach when it is further shared with others.[91] People also exist in different social spheres, often keeping their work and home lives separate. Information known by all of a person's friends is not *secret*, but it is reasonable to expect in many situations that a person's employer will not find out. As a society, information is not "public" or "private"; it is not even on a single spectrum. The only way to describe the work/home separation is to describe the flow of information: whom it is kept *from* or told *to*. Lacking that information, it is impossible to determine whether a person's privacy has been breached. Additionally, like the public/private distinction, courts do not even follow the third-party doctrine to its logical conclusion.[92]

Under current Fourth Amendment doctrine, when a court is faced with a problem that seems to defy the narrative, it must choose one of two options. Either it sticks with the binary rule in a way that bears little

---

87 *See* United States v. Jones, 132 S. Ct. 945, 951–52 (describing prior doctrine as permitting law enforcement monitoring when information has "been voluntarily conveyed to the public").

88 *See, e.g.*, *Breaking Bad: Buyout* (AMC television broadcast Aug. 19, 2012) (Attorney Saul Goodman tells DEA agents that following his client for three days amounts to stalking, for which he could obtain a TRO, while conceding that it is not technically a Fourth Amendment violation. In the next scene, Goodman admits to his client that the TRO application would be rejected in court as the law stands now.).

89 *Cf.* Terry v. Ohio, 392 U.S. 1, 27 (1968) (recognizing a "narrowly drawn" exception to searches on the street, permitting a frisk where the officer "has reason to believe that he is dealing with an armed and dangerous individual").

90 Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) ("The rule is simple: By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed.").

91 *See id.*

92 Strandburg, *supra* note 32, at 642 ("[C]ourts are increasingly disinclined to take a simplistic and aggressive third party doctrine approach. . . . [T]he few appellate opinions to consider the issue have found that Fourth Amendment protection extends to the content of digital communication despite intermediary storage." (footnotes omitted)).

resemblance to society's privacy values, such as in the third-party doctrine, or it must find a new distinguishing feature. The court will then seize upon that distinction to create a new binary rule. This is what happened in *Jones*.[93] Some of the Justices retreated to property law, punting the privacy question, but the other Justices could not characterize what went wrong with their previous decisions and instead opted for a new, binary rule: following someone for a long time via GPS is a search.[94] This left a huge number of questions: How long is too long?; What about other technologies, like cell site tracking or drones?[95] Eventually these questions will be answered with more binary rules.

With the focus on binaries, the doctrine is incapable of doing anything but creating a never-ending series of finer distinctions.[96] Eventually, with enough iterations, the resulting doctrine might cover so many different situations that it could approximate a doctrine focused on social contexts, but the results could just as easily make no sense because they would have no theoretical cohesion.[97] Search doctrine need not be so random. Contextual search helps explain the relationship between each seemingly different fact pattern and provides the missing bigger picture.

B. *The Circularity of* Katz

The circularity of *Katz* is a well-known logical trap that, when sprung, threatens to erode privacy entirely. The trap is simple: If a person knows she is being watched, she cannot reasonably expect not to be watched. Of course this would mean that if a new policy of total surveillance were announced and widely publicized, there would be no recourse against it, because a belief that a person was not being observed would be objectively unreasonable. Call this idea "objectively reasonable subjectivity." To fall into this trap is to commit an is-ought fallacy by conflating the descriptive expectation in the subjective test with the normative one in the objective test, better termed a "privacy interest."

The fly-over cases discussed earlier demonstrate the Court's exacting approach to this idea.[98] The Court also returned to this doctrine in *Kyllo v. United States*,[99] implying that once a privacy-

93 *Jones*, 132 S. Ct. 945.

94 *Id.* at 961 (Alito, J., concurring).

95 *See, e.g.*, Benjamin J. Priester, *Five Answers and Three Questions After* United States v. Jones (2012)*, the Fourth Amendment "GPS Case"*, 65 OKLA. L. REV. 491, 519–29 (2013).

96 *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479–80 (2011).

97 *Id.*

98 *See supra* text accompanying notes 70–71.

99 533 U.S. 27 (2001).

defeating technology becomes commonplace, people cannot reasonably expect that it will not be used, and therefore will have no privacy expectation.[100]

The conflation originated with Justice Harlan's concurrence itself. Though the *Katz* test is often quoted as whether a litigant has a "reasonable expectation of privacy," Justice Harlan's concurrence stated something a little different: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[101] Justice Harlan continued:

> Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[102]

In both of these examples, the speaker is deciding the level of control to exercise over his speech. For "conversations in the open," society is unwilling to recognize a privacy interest precisely *because* none has been claimed. The confusion is partly an unfortunate result of the use of the word "expectation" in both halves of the test.[103] The word "expectation" can mean both "demand" and "predict."[104] There is a meaningful difference between what people in society have a *right* to expect of police behavior and what is descriptively predicted.[105]

---

100 *Id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained . . . constitutes a search—at least where (as here) the technology in question is not in general public use." (citation omitted)).

101 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

102 *Id.*

103 "Justice Harlan himself later expressed second thoughts" about the word "expectation," due to the circularity problem. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

104 Merriam-Webster defines "expect" in three relevant ways, with the last two being equivalent for these purposes: "[(1)] to consider probable or certain <*expect* to be forgiven> <*expect* that things will improve>[; (2)] to consider reasonable, due, or necessary <*expected* hard work from the students>[; and (3)] to consider bound in duty or obligated <they *expect* you to pay your bills>[.]" MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 408 (10th ed. 1999). "Predict" is a related word. *Id.*

105 Some of the confusion might also be derived from the terms "objective" and "subjective." "Objective" and "subjective" here mean "reasonable person" versus "individual," as they do in other areas of law utilizing a reasonable person standard. If one thinks of the terms in a different sense, however, as "objective evidence" versus "subjective emotion," the term "objective" begins to look like objectively reasonable subjectivity. That is, actual evidence shows that privacy is not being protected; therefore it is irrational, emotional, or unreasonable to

Justice Harlan's subjective/objective duality is not defective; it is just not the general case. His example only covers cases in which *control* is the relevant transmission principle. The phrase "conversations in the open" refers to a person who is choosing not to hide information with the background assumption that had she done so, the information would have been protected; this is the *control* transmission principle.[106] *Control*, however, is a special case. Where *control* is the transmission principle, waiver is possible. If a person waives the right to privacy by having a conversation in the open, society does not recognize a right to protect that information *because* she waived that right, and for no other reason. Thus, the "subjective" and "objective" converge because it is objectively unreasonable to protect a right that the person waived. In contextual integrity terms, though, the key is that because the person shared the information willingly, the informational norm was not breached. In the general case, privacy is violated if and only if the informational norm is breached.

Contextual search implements the twofold requirement as two separate steps, inherently avoiding the conflation. The objective inquiry translates to the framework analysis. In the framework analysis, the theory analyzes the context to ask, "Does society recognize an expectation of privacy here?" It answers the question by describing the expected information flows, which are based on informational norms. The framework analysis makes no reference to the events in question; it considers only the background social norms. The subjective expectation, on the other hand, is folded into the violation inquiry, though the violation inquiry is only subjective in the degenerate case of *control*. Thus, if a person knowingly exposes information for which the transmission principle says he has *control*, then the receipt of that information does not violate contextual integrity. This is the difference between whispering a secret to a friend and yelling it across the room.

By generalizing to informational norms, the two halves can be parsed. Consider again the medical context and bullet wounds. The existence of mandatory reporting laws is not enough to tell if reporting is the informational norm (though it is good evidence), so the transmission principle is unknown. The transmission principle could either permit that information flow, or it could not. Therefore, whether it is a violation for police to receive the information will depend on which way the informational norm points; if the norm is reporting, there will be no violation, and vice versa. There is nothing subjective about this case and waiver is not a factor, but the Fourth Amendment violation still turns on the informational norm. That is because

believe that it is. I do not know if this misconception is fueling the confusion, but it is something to think about.

106 NISSENBAUM, *supra* note 24, at 69–71.

control—a subjective choice—is not the relevant transmission principle. It is the breach or non-breach of the norm that is the more general case, and subjectivity is not always present.

C. *State Action and the Artificial Meaning of "Search"*

As any confused law student in Criminal Procedure can tell you, current Fourth Amendment doctrine defines a "search" in a way that is at odds with the English language. If police are riding down the street in a patrol car looking for a suspect, English speakers would naturally say that the police are "searching" for someone, but the Fourth Amendment disagrees. The net effect of this linguistic distortion is that instead of a restraint on government power, many see the Fourth Amendment as a grant of such power.

This linguistic shift seems to have originated from the plain view doctrine, the sentiment that "police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public."[107] The plain view doctrine makes sense, but in its purest form it is nothing more than a restatement of the "action" part of the state action requirement.[108] If the police are not actively seeking information and just happen to witness a crime or stumble upon evidence, then the Fourth Amendment is not implicated *because there is no state action*, regardless of the definition of search.[109] Similarly, if a criminal co-conspirator decides to become an informant of his own volition, there is no state action, and the Fourth Amendment is not implicated. In current doctrine, however, even where there is police action, either to actively seek evidence or to convince a suspect to turn informant, current doctrine still says there was no "search."[110] Thus, entire classes of police investigative tactics are eliminated from the Fourth Amendment's purview with little justification.[111]

The role of state action in the Fourth Amendment is suppressed because of how the law defines "search." It has actually become dogma that police cannot have *less* access to information than the average person.[112] The individual rights provisions of the Constitution, however,

---

107 California v. Greenwood, 486 U.S. 35, 41 (1988).

108 United States v. Jacobsen, 466 U.S. 109, 114 (1984) (stating that the Fourth Amendment requires state action).

109 This is different than the case when the police are looking for one piece of information and inadvertently find something else, as discussed in *Horton v. California*, 496 U.S. 128, 134 (1990). In this type of case, state action is clearly present, but norms are not violated when police find additional evidence in plain view; so there is a search, but no violation.

110 Hoffa v. United States, 385 U.S. 293 (1966).

111 *See infra* Parts III.A–B.

112 *See, e.g.*, *Greenwood*, 486 U.S. at 40 (reasoning that police should have access to garbage left on the sidewalk because they "are readily accessible to animals, children, scavengers,

function as a restraint on government power.[113] State action doctrine, as a general matter, serves the purpose of limiting government action as compared to actions by citizens.[114] The canonical example is the dinner guest hypothetical, which says that while a private citizen may hold dinner parties that are racially segregated, the government may not segregate a public building.[115] Because state action is indisputably relevant in the Fourth Amendment,[116] there is no a priori reason why permitted acts of searching should not be *more limited* for a government actor than for a private citizen. In fact, for the Fourth Amendment to work similarly to other constitutional provisions, police *must* have less access to information than private citizens can.[117] Obscuring these limitations is the prime effect of the linguistic abuse of the word "search" in current doctrine.

Contextual search disentangles the concepts of "search" and "reasonable expectation of privacy." Here, because the entire concept of a "reasonable expectation of privacy" is defined by contextual integrity, the definition of search must mean something else. "Search" is thus returned to its English language definition: "to look into or over carefully or thoroughly in an effort to find or discover something,"[118] or in the parlance of this Article, a person's intentional act of seeking to change information flows in order to receive more information.[119] Under contextual search, a Fourth Amendment violation occurs when a search (intentional act to change information flows) by a state actor causes a contextual integrity violation (violation of the reasonable

snoops, and other members of the public" (footnotes omitted)); California v. Ciraolo, 476 U.S. 207, 218–19 (1986) (reasoning that because any member of the public could see something, then the officers necessarily should be permitted to as well).

113 *See* Wilson R. Huhn, *The State Action Doctrine and the Principle of Democratic Choice*, 34 HOFSTRA L. REV. 1379, 1387 (2006) (discussing the difference between powers/structural provisions and rights provisions of the Constitution).

114 DeShaney v. Winnebago Cnty. Dep't of Soc. Servs., 489 U.S. 189, 196 (1989) ("[The Fourteenth Amendment's] purpose was to protect the people from the State, not to ensure that the State protected them from each other.").

115 *E.g.*, G. Sidney Buchanan, *State Authorization, Class Discrimination, and the Fourteenth Amendment*, 21 HOUS. L. REV. 1, 10 (1984); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 538 (1985).

116 United States v. Jacobsen, 466 U.S. 109, 114 (1984).

117 *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1416 (2013) ("[A] police officer not armed with a warrant may approach a home and knock, precisely because that is 'no more than any private citizen might do.'" (quoting Kentucky v. King, 131 S. Ct. 1849, 1862 (2011))).

118 MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1053 (10th ed. 1999).

119 Kyllo v. United States, 533 U.S. 27, 32 n.1 ("When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" (alteration in original) (citing NOAH WEBSTER, AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828), *available at* http://archive.org/stream/americandictiona02websrich#page/n540/mode/1up)); *see also* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 24 (2007) (advocating a similar definition of search).

expectation of privacy). This is consistent with the *Katz* doctrine in its original form, which would have found a Fourth Amendment violation where a state actor violated a reasonable expectation of privacy.

Restoring the definition of search in this way would render a great deal more police activity searches, but under this theory, the search does not by itself imply a violation or require a warrant. A search that comports with informational norms is by definition a reasonable search. For example, if the police went to a suspect's house to look for evidence, and that evidence happened to be lying on the suspect's front lawn, the legal conclusion would be the same under both theories, but contextual integrity calls it a reasonable search while current doctrine does not call it a search at all. A stakeout would have a similar result—it would be considered a search, but it is eminently reasonable as a relatively unobtrusive police tactic. The result is that the same conceptual space is covered between the two theories, but structure of the reasoning is different. Figure 1 explains the analytical structure change.

A second difference between the analytical structure of contextual search and current doctrine is that warrants and warrant exceptions are encoded as part of transmission principles, seen in Figure 1 as part of the descriptive analysis.[120] So in the case that the police go to the suspect's house with a warrant, it is a reasonable search because it comports with transmission principles—specifically, that police may receive the specific information with a valid warrant.[121] Thus a warrant is just one possible element of determining a reasonable search. Under this theory, it cannot be determined whether a reasonable expectation of privacy was violated without the information about whether a warrant has been obtained; it is all one step. Recall, though, that the text of the Fourth Amendment never mentions "searches" as a standalone concept.[122] Rather, it only addresses "unreasonable searches."[123] Thus, a single query about whether a particular police action was an unreasonable search is truer to the text as well.[124]

120 Warrants become part of the transmission principle because of contextual search theory's stare decisis. The judgment that warrants permit information transfer dates at least back to the drafting of the Fourth Amendment. If we lived in a society in which warrants did not exist, but the society nonetheless believed that limited warrants *should* exist, the contextual search analysis would determine that warrants should exist, then contextual search's stare decisis element would preserve that outcome.

121 YALE KAMISAR ET AL., MODERN CRIMINAL PROCEDURE 305–06 (11th ed. 2005) (discussing the particularity requirements of warrants).

122 U.S. CONST. amend. IV.

123 *Id.*

124 Amar, *supra* note 65, at 759.

Analytical Placement of Key Questions in Current Doctrine and Contextual Search

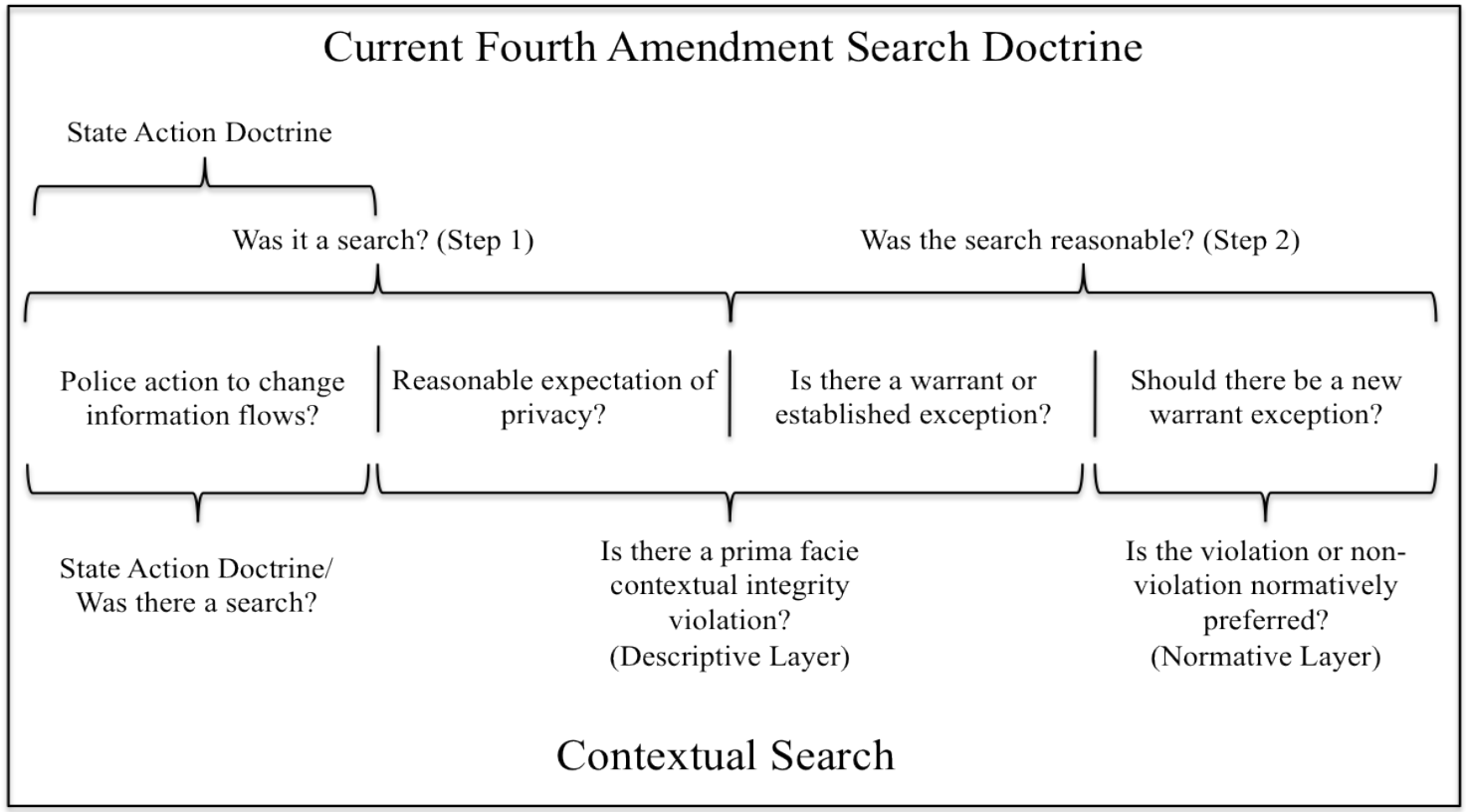

Figure 1

D. *Lack of Clarity in the Normative Test*

The reasonableness question in current doctrine is subject to a great deal of hand waving and loose reasoning.[125] Two questions are asked simultaneously—whether there *is* a warrant exception and whether there *ought to be* a warrant exception. This makes it very easy to expand the exceptions by creating new exceptions that are similar to the old ones, without necessarily thinking of them as new.[126] The doctrine has thus slowly crept along throughout time, excluding ever more situations and police tactics from warrant requirements. Contextual search, however, shunts the entire inquiry about the *current* state of the law to the descriptive analysis, so only the normative question remains: Should the outcome of the descriptive layer stand as is?

The normative structure of contextual integrity aids this process by more specifically identifying the particular values at stake in each decision. In the current paradigm, the normative question is doctrinally limited to the values of the law enforcement context.[127] Nonetheless, in some cases, courts appear to consider some of the values of their particular contexts.[128] Contextual search asks judges to systematize those considerations. This is appropriate because the social contexts are so foundational to society that preservation of these contexts should be an equal goal to enabling police action.[129]

Generally, applying contextual integrity's normative analysis in Fourth Amendment cases is easier than in more open-ended settings because the Fourth Amendment is itself a normative statement defining many of the values at stake. Depending how the law enforcement context is defined, various values include enabling the police to better perform their jobs, the liberty of citizens in their interaction with police, and community cohesiveness. These same values will appear again and

---

125 Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 978 ("[T]he reasonableness analysis employed by the Supreme Court has repeatedly changed and each new case seems to modify the Court's view of what constitutes a reasonable search or seizure.").

126 See, for example, the discussion of the transition from the informant cases to the informational third-party doctrine, *infra* Part III.B.

127 *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) ("On one side of the balance are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order.").

128 For example, see *T.L.O.*, 469 U.S. at 338–40, a case about warrantless searches of students in school. After stating that the issue is to balance individual rights and law enforcement objectives, the opinion additionally considers the educational context: "How, then, should we strike the balance between the schoolchild's legitimate expectations of privacy and the school's equally legitimate need to maintain an environment in which learning can take place?" *Id.* at 340.

129 *See* NISSENBAUM, *supra* note 24, at 127.

again in these cases because that is the nature of the normative Fourth Amendment inquiry. Thinking about social contexts this way, a warrant can be seen as a judicial determination that law enforcement values take precedence over other social values in the particular situation in which a warrant was granted. This is why the proper transmission principle across contexts will often include permission for information to flow to police with a warrant.

Beyond recognizing warrants as a trump card, identification of the various values at stake in the overlapping contexts is as far as the theory can go. At some point, normative judgments weighing those values must be made, but identifying the values correctly makes it easier to gather empirical evidence of people's views[130] or to have meaningful debates anchored in some other source of ethical reasoning.

III. OPERATIONALIZING CONTEXTUAL SEARCH

This section addresses several cases and areas within search doctrine to illustrate both how to analyze a case under contextual search and how the doctrine would eventually look if interpreted this way. The selection of cases and doctrines is not meant to be exhaustive, but rather is intended to show how contextual search either matches or changes some of the basic parts of search doctrine.

There are two types of cases for which current doctrine and contextual search are in clear agreement. These cases represent the extremes: plain view doctrine and blatant violations, such as police officers breaking into a suspect's home looking for evidence without a warrant. As discussed earlier, the plain view doctrine is essentially the requirement that the police search for information (in the plain English sense) before the Fourth Amendment is implicated.[131] At the other extreme, unjustified police entry violates both standard Fourth Amendment doctrine and contextual integrity for essentially the same reason. As a matter of current law, courts have said that the "home" is such a quintessentially private place that physical intrusion even by a "fraction of an inch" is too much.[132] Contextual search would instead say that the home is a specific social context. As against the police, the contents of one's home are subject to the transmission principle of

130 *See, e.g.*, Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy"*, 11 U. PA. J. CONST. L. 331 (2009); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727 (1993).

131 *See supra* Part II.C.

132 Kyllo v. United States, 533 U.S. 27, 38 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

control by the resident, flowing to police with a warrant or warrant exception. Thus the unjustified entry is a prima facie violation, and the discussion moves to the normative layer. A rule that police could simply break into houses at any time would lead to the complete breakdown of trust between the citizenry and government and would be ripe for abuse, encouraging all the things the Fourth Amendment was designed to prevent. Additionally, it would destroy the home as a social institution, generally seen as the one place it is always safe to retreat. The normative layer therefore finds that the old rule is more desirable. It is not surprising, either, that the home would generate a consensus between the two theories because the home itself is both a spatial context, with which the Fourth Amendment was originally concerned, and a social context—contextual integrity's arena.[133]

The discussion in this Part focuses on more difficult cases and doctrines: third-party doctrine, including cases involving information released to third parties and the use of informants;[134] cases expressing the idea of "no privacy in public;" emanations; and dog sniffs, all of which are dismissed as "not a search" under current doctrine.[135] There is also a short section on roving wiretaps, which are more easily justified under contextual search than current doctrine.[136]

The cases are analyzed here by examining the particular information flows at stake and resolving the questions in a way the Court was often simply unable to do without a context-based theory. Contextual integrity is a very different looking analysis than most, but the conclusions in this section echo the critiques of many other Fourth Amendment scholars. The benefit here is that the resulting structure is all derived from a single underlying theory.

A. *Information Relayed to Third Parties*

The third-party doctrine is the favorite villain of many Fourth Amendment scholars.[137] Originating from two cases, *United States v. Miller*[138] and *Smith v. Maryland*,[139] the doctrine states that there is no expectation of privacy in information knowingly disclosed to a third

133 *See infra* Part V.A.

134 Third-party doctrine, as commonly understood, consists of two separate sets of cases: cases involving information released to a third party and informant cases. Kerr, *supra* note 90. The doctrines are considered separately and should not be confused, despite their similarities.

135 *See infra* Parts III.A–D.

136 *See infra* Part III.E.

137 Kerr, *supra* note 90 ("The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner* of search and seizure law, widely criticized as profoundly misguided." (footnote omitted)); *id.* at 563 n.5 (collecting critical writings).

138 425 U.S. 435 (1976).

139 442 U.S. 735 (1979).

party.[140] The Court ruled in *Miller* that there was no Fourth Amendment interest in bank records, because the records had been exposed to a bank, and thus were no longer private.[141] In *Smith*, there was no privacy interest in the phone numbers a person dialed because they were similarly exposed to the telephone company.[142] Criticisms of these decisions abound,[143] and the doctrine may be falling into disfavor with the Court.[144] Nonetheless the doctrine is frequently relied on by law enforcement.[145]

This is one of the simpler doctrines to examine with contextual search, as an in-depth look at *Miller* demonstrates. The facts of *Miller* are as follows: Mitch Miller was suspected of operating an illicit distillery, and as part of their investigation, agents from the Bureau of Alcohol, Tobacco, and Firearms (ATF) issued a subpoena for "all records of accounts, *i.e.,* savings, checking, loan or otherwise, in the name of Mr. Mitch Miller."[146] The bank then gave all the records to the police, without telling Miller about the subpoena.[147] Eventually, on the strength of those records, Miller was convicted.[148]

At trial, Miller moved to suppress the records, and the district court denied the motion.[149] The Fifth Circuit reversed, stating it was Miller's privacy—rather than the bank's, at stake—and thus the bank had no right to consent to a search.[150] Eventually the Supreme Court reinstated the district court's decision.[151] Miller argued that "he ha[d] a Fourth Amendment interest in the records kept by the banks because they [we]re merely copies of personal records that were made available to the banks for a limited purpose."[152] The Court rejected that argument, saying that "in *Katz* the Court also stressed that '(w)hat a

140 Kerr, *supra* note 90.

141 *Miller*, 425 U.S. at 445.

142 *Smith*, 442 U.S. at 745–46.

143 Strandburg, *supra* note 32, at 616 n.10 (collecting critical writings).

144 *Id.* at 615, 617 (observing that the Court ignored the third-party doctrine in *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), a case that could easily have been decided on that basis); *see also* United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

145 FBI, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE §§ 18.7.1.3.4.4 (2012), *available at* https://www.aclu.org/files/pdfs/email-content-foia/FBI%20docs/June%202012%20FBI%20DIOG.pdf.

146 *Miller*, 425 U.S. at 437 (internal quotation mark omitted). The subpoena was cited as "allegedly defective," but the Court specifically ruled irrespective of the subpoena's validity. *Id.* at 436, 440.

147 *Id.* at 438.

148 *Id.*

149 *Id.*

150 *Id.* at 439.

151 *Id.* at 440.

152 *Id.* at 442.

person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'"[153]

Under contextual search, that exchange is the crux of the matter. The formal analysis of *Miller* begins with the framework—the actors, attribute, and transmission principle. Who are the actors (subject, sender, receiver)? The information at issue relates to the defendant, so he is the subject. The information is held by the bank, the sender, and given to the police, the receiver. The attribute is financial information—the checks and deposits named in the motion to suppress.[154] Finally, consider the transmission principle. Banking customers give checking information to banks that they would not want the public to know; people generally do not share account numbers, or information about balances, payments, or deposits. Customers share with the bank because it needs to track that information to provide its essential services. When banks share information with outsiders even accidentally, people are often outraged enough to switch banks or file lawsuits.[155] Outrage is always a good piece of evidence for a transmission principle.[156] Thus the transmission principle could be stated as strict confidentiality in banking information, except sharing necessary for banking purposes, with consent from the subject (e.g., to an accountant), or to the police with a warrant.[157]

The framework establishes that there was a reasonable expectation of privacy in this type of information (banking records) flowing between these actors. Next, the theory asks: given this framework and the facts, was there a violation? The answer is yes. The police did not have a warrant and there was no established warrant exception, yet they obtained the information from the bank.[158] The remainder of the inquiry is in the normative layer: Should a rule permitting the police to obtain banking records with only the consent of the bank become the

153 *Id.* (alterations in original) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

154 The bank also had contact information, such as name, phone number, and address, but a different transmission principle guides this information. *Id.* at 440–44. Here the state convicted on the strength of the bank records, not because the police used the contact information to track Miller down, so the bank records are the relevant information. *Id.*

155 Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation* 3 (Temple Univ. Legal Studies Research Paper No. 2012-30, 2013) (forthcoming in J. EMPIRICAL LEGAL STUD.), *available at* http://papers.ssrn.com/sol3/papers.cfm? abstract_id=1986461 ("[T]he odds of a firm being sued as a result of improperly disposing data are . . . 6 times greater when the data breach involved the loss of financial information.").

156 *See supra* Part I ("People's indignation, anxiety, fear, anger, and outrage over a privacy violation are evidence that an informational norm has been breached, and protest and resistance often follow.").

157 Recall that with a warrant, the law enforcement context has been judged the most salient context, and the police may have access to information in the warrant. *See supra* note 120.

158 If the bank had independently noticed that the accounts were odd and handed over the documents, there would have been a contextual integrity violation, but no Fourth Amendment violation because there was no state action; the police would not have been searching.

new norm? At the margins, surely, money would flow less freely in society with this new norm than without it, though the banking system did not collapse when this case was decided in 1976. But more than practical survival in the banking context is at issue. The values inherent in that context must be addressed, leading to the question: Is it "in our society's interest to condition a [c]onsumer's use of the nation's banking system on a waiver of his Fourth Amendment privacy[?]"[159] The normative analysis has to balance the harm to the values in the banking context, including what people are forced to give up for access, against the aid to law enforcement of warrantless access to the records. This is as far as contextual search can go. The specific answer requires an ethical debate regarding those principles.

Regardless of whether the *Miller* outcome was correct, the effect of leaving out a conscious consideration of context in this case was to plant the seeds of a sweeping exception to Fourth Amendment protection where it made no sense to do so. The most important fact was that Mitch Miller gave the documents to the bank "for a limited purpose."[160] After balancing the interests, a court could have concluded in a context-conscious ruling that harm to the banking system was minimal and the police should have access to the documents. This would have the same outcome for Miller as a defendant, but a context-conscious ruling could not have created the third-party doctrine as a blanket rule.

In fact, the Court was not completely oblivious to the importance of context. The Court made four more statements after the announcement of the third-party doctrine as a general proposition, at least the first and third of which betray an awareness of context:

> (1) "[I]f we direct our attention to the original checks and deposit slips . . . we perceive no legitimate 'expectation of privacy' in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions."
>
> (2) "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."
>
> (3) "The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they 'have a high degree of usefulness in criminal tax, and regulatory investigations and proce--edings.'"

---

159 Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 242 (2006).

160 United States v. Miller, 425 U.S. 435, 442–43 (1976).

> (4) "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[161]

Statement (1) suggests that confidential communications would be entitled to privacy protections, but that the documents in question were just "negotiable instruments," ignoring the sensitive nature of much of the included information. The statement suggests a requirement of *explicit* confidentiality in privacy protections, which is at odds with the concept of a "reasonable expectation of privacy." A person would only *explicitly* agree to privacy beforehand in situations where it is otherwise unreasonable to *expect* privacy; if privacy expectations are reasonable, no one would think a confidentiality agreement necessary. Thus the reasoning is completely circular. Statement (1), with its awareness of context, also seems inconsistent with the third-party rule stated just a few sentences earlier.[162]

Statement (2) is definitely true, but it implicitly equates exposure to the bank for limited purposes with exposure to the public at large. Miller conceded the voluntariness of the disclosure, but it was not at issue.[163] If the transmission principle were to control, rather than confidentiality, the voluntariness of the disclosure would have been at issue. A control transmission principle is only reasonable if the bank's privacy is at issue, because then the subject and sender would be the same entity—the bank—and the transmission principle of *confidentiality except with consent* becomes *control*. Here, as the Fifth Circuit and Justice Brennan noted, that was not the case.[164] This is why the Court missed the real issue: the difference between exposure of information to a bank and the public at large.

Statement (3) is simply false, or at the least, unsupported. The statement claims that Congress, by requiring preservation of documents, foresaw and permitted a transfer of information from one context to another—banking to law enforcement. While it is true that Congress likely did foresee such a transfer, the statement does not support the idea that Congress has authorized it without any form of process. Congress could have easily assumed that the relevant transmission principle was access with a warrant, not open sharing.

---

161 *Id.* (citations omitted).
162 *Id.* at 442.
163 *Id.* at 439–42.
164 *Id.* at 450 (Brennan, J., dissenting).

Statement (4) connects the information-based third-party doctrine with precedent from the cases involving informants.[165] The Court had previously stated that a person takes a risk when disclosing information to someone who might potentially be an informant.[166] However, to apply the same reasoning to a highly-regulated institution, which society depends[167] on for confidentiality, betrays insensitivity to context that would not have been possible under a contextual analysis. The informant cases place the onus on people to be careful choosing their friends,[168] but to place those same conditions on a relationship with a bank is inconsistent with social norms for that context, in which people are supposed to trust their institutions.

Smith v. Maryland[169] has the same problems as *Miller*. In *Smith*, the Court held that because the phone numbers are relayed to the phone company they are no longer private.[170] As in *Miller*, this equates the employees of the phone company—who are in a specific, limited relationship with the defendants—with the public at large. Normatively, the Court should have asked if it is in society's interest to condition telephone use on the waiver of Fourth Amendment rights, much as it conditioned bank use.

The danger of the doctrine is even more apparent today, as society relies on digital communications in which every action is transmitted to third-party Internet service providers, search engines, email servers, and others. A context-insensitive rule that all this information is public makes many people uncomfortable (including Justice Sotomayor),[171] and perhaps that is why the doctrine may be on shaky ground.[172]

B. *Informants and "Pretend Friends"*

Some of the flaws in the third-party doctrine stem from its reliance on the equally flawed informant cases.[173] In these cases, a police officer gathers information either by going undercover and becoming a "pretend friend"[174] or convincing a prior confidant of the defendant to betray him. The Court's view in these cases is that "'no interest legitimately protected by the Fourth Amendment is involved,' for that

165 *See infra* Part III.B.

166 *Miller*, 425 U.S. at 440 (citing Hoffa v. United States, 385 U.S. 293, 301–02 (1966)).

167 *Id.* at 451 (Brennan, J., dissenting) ("[I]t is impossible to participate in the economic life of contemporary society without maintaining a bank account.").

168 *Id.* at 440 (majority opinion) (citing *Hoffa*, 385 U.S. at 301–02).

169 442 U.S. 735 (1979).

170 *Id.* at 742.

171 United States v. Jones, 132 S. Ct. 945, 957 (2012).

172 *See supra* note 144.

173 *Miller*, 425 U.S. at 440 (relying on *Hoffa*, 385 U.S. at 301–02).

174 Colb, *supra* note 66, at 139.

amendment affords no protection to 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.'"[175] The Court has failed to distinguish between three different informant scenarios. In the first, the prior confidant/co-conspirator has a change of heart and confesses the entire enterprise with no prompting from the police. In the second, the police turn the confidant, perhaps, but not necessarily, in exchange for immunity. In the third, the police go undercover and form a new relationship with the target of the investigation, earning his trust.

The differences between the three scenarios are the actions of the police officers involved. Under current doctrine, none of the scenarios amounts to a search, but the information flow is different in each one, and so each should be examined separately. The first scenario requires no action at all by the police, and thus it would not implicate the Fourth Amendment under either current doctrine or contextual search. This is also why the first scenario never appears in the governing cases: there is no state action. The second and third scenarios do contain state action, however, so the information flows must be examined.

In *Hoffa v. United States*,[176] the police convinced an incarcerated former associate of Jimmy Hoffa's to become an informant in exchange for dropping the charges against him.[177] When Hoffa then told his former associate incriminating information, the associate reported it to the police, and Hoffa was convicted based on that information.[178] There are two relevant information flows here: Hoffa to associate and associate to police. The first was not new—Hoffa and the associate shared information constantly—and the flow does not involve the police, so only the second flow raises concerns. In the second flow, Hoffa is the subject, the associate is the sender, and the police are the receivers. The attribute is the incriminating information: in this case conversations about jury tampering.[179] The relevant transmission principle would be that a person does not rat on his friends or associates.[180] The associate should *withhold* information in this case.

In *Lewis v. United States*,[181] a police officer misrepresented his identity as someone who had an interest in buying drugs[182]—the

175 United States v. White, 401 U.S. 745, 749 (1971) (quoting *Hoffa*, 385 U.S. at 302).

176 385 U.S. 293 (1966).

177 *Id.* at 298.

178 *Id.* at 294–95.

179 *Id.*

180 A common objection could be raised here: that the "criminal conspiracy" context should be considered separate, and one in which society would grant police more access. This puts the cart before the horse. The Fourth Amendment applies equally to all, and the whole point is that whether people are criminals is unknown ahead of trial. Therefore, while prison might be its own context, *see infra* Part V.A, labeling someone a part of the criminal context before conviction is circular.

181 385 U.S. 206 (1966).

simplest of undercover work. Here, the context seems undefined. Lewis thought it was a standard business transaction, but the police officer knew the business context was false.[183] However, if someone represents himself as a part of one context, he should be estopped from violating that context's norms. Someone, for example, who pretends to be a doctor, certainly does not get to take *more* liberty with a would-be patient's information than a real doctor. The same is true here. So the subject and sender in this case is Lewis; the officer is the receiver. The attribute is the fact that Lewis sells drugs. The transmission principle is that a potential seller shares that information freely with a buyer, but it is withheld from the public, especially police.

In both these cases, the transmission principle is different between co-conspirators than it would be between police and a single co-conspirator, and thus the information flow is changed by the actions of police. The normative layer then asks whether warrantless undercover police work is worth the cost to the fabric of social relationship in society.[184] At the margins, if people believe that neighbors, friends, employers, or clients could be reporting to the police, these relationships will suffer. If people believe that the police could pressure friends to report on them, they would likely shy away from those discussions or those associations that might put them on the police's radar. The fact that most people do not spend their time worrying about this now reflects the fact that this sort of suspicionless infiltration of social groups is only likely to take place within already marginalized parts of the population. For example, take last year's revelation that the NYPD infiltrated Muslim Student Associations throughout the tri-state area,[185] based on the strange rationale that police merely go where there are "allegations."[186] The result, predictably enough, was that students in these groups began to avoid talking about politically sensitive subjects, if they managed to get past the pressure from their families urging them not to join at all.[187] If the rule is instead that police at least must have

182 *Id.* at 206–07.

183 *Id.* at 207–08.

184 Here we are merely discussing suspicionless undercover work, which is what the Court ruled permissible. *See id.* at 208–10.

185 Chris Hawley, *NYPD Spied on Muslim Students at Yale, All over the Northeast*, HUFFINGTON POST (Feb. 20, 2012, 4:35 AM), http://www.huffingtonpost.com/2012/02/21/nypd-spied-on-muslim-stud_n_1290544.html.

186 Al Baker & Kate Taylor, *Mayor Defends Monitoring of Muslim Students on Web*, N.Y. TIMES, Feb. 22, 2012, at A18.

187 Arun Venugopal, *Muslims Say NYPD Surveillance Is Already Changing Behavior*, WNYC NEWS (Feb. 29, 2012), http://www.wnyc.org/blogs/wnyc-news-blog/2012/feb/29/muslims-say-nypd-surveillance-already-changing-behavior; *see also* MUSLIM AM. CIVIL LIBERTIES COAL., CREATING LAW ENFORCEMENT ACCOUNTABILITY & RESPONSIBILITY PROJECT & ASIAN AM. LEGAL DEF. & EDUC. FUND, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), *available at* http://aaldef.org/Mapping%20Muslims%20NYPD%20Spying%20and%20its%20Impacts%20on%20American%20Muslims.pdf.

individualized suspicion, if not a warrant, to invade social circles, then people can worry less that police would pressure their friends for improper reasons, such as a religious affiliation.[188]

The winning arguments in the *Hoffa* and *Lewis* cases took the form of an "assumption of the risk" rationale: people should be careful of whom they trust, and if confidants turn on a person or were never a real friend in the first place, the information is fair game.[189] This rationale, like the extension of plain view doctrine, ignores the actions of the police and does not support the outcomes it is meant to. The "assumption of the risk" rationale protects only people that can be said to have a perfect "traitor detector" and thus can stop speaking to those who they do not trust.[190] There is also a substantive difference between spontaneous treachery and police coercing or even cajoling someone into betraying his friend, just as there is a difference between a phone confession to police and a wiretap. The failure to consider police action turns a Fourth Amendment question into victim-blaming.[191]

The Court can be forgiven for deciding *Hoffa* and *Lewis* the way it did, because both came a year before *Katz* made a "reasonable expectation of privacy" the touchstone for Fourth Amendment searches. However, four years after *Katz*, the Court decided *United States v. White*,[192] extending the holding of *Hoffa* to include situations where the informant was wearing a wire and declaring that *Katz* left informant doctrine unchanged.[193] This is odd when one considers that both cases involved a hidden electronic device relaying information back to the police.[194] At least the similarities warranted more than a cursory dismissal, but in the end the court stuck with the "traitor detector" rationale of *Hoffa* and *Lewis.* The Court then reasoned that there was no difference between the informant hearing the information then telling

188 Such a rule would not "severely hamper undercover investigations," as Orin Kerr fears, because the required level of suspicion can differ with specific context. *See* Kerr, *supra* note 90, at 568. Beyond the dividing line of *some* suspicion or *none*, the specific level of suspicion required in each case is beyond the scope of this Article—all contextual search doctrine says is that *some* should be required.

189 Hoffa v. United States, 385 U.S. 293, 302 (1966); Lewis v. United States, 385 U.S. 206, 212 (1966).

190 Colb, *supra* note 66, at 142. To borrow Professor Colb's analogy, whether a person has a home alarm system or not makes it more or less likely that his home will be burglarized, but if and when a home without an alarm system is burglarized, the burglar certainly has no defense that the home was not alarmed; the burglar is equally blameworthy either way. Ignoring police action in inducing the treachery is equivalent to ignoring the actions of the burglar and basing the violation on whether the residents were being careful enough.

191 *Id.*; *see also* Amsterdam, *supra* note 103, at 406–07 (analogizing to the inherent risk of parking a car in Greenwich Village, New York City).

192 401 U.S. 745 (1971).

193 *Id.* at 749.

194 Colb, *supra* note 66, at 141.

the police and it being relayed electronically in the first place.[195] Of course, even accepting the previous informant doctrine, by now it should be obvious that there is a difference, whether or not it ends up being significant enough to matter. Information flows are disrupted by the act of recording or electronically transmitting information, and people tend to be quite disturbed when they find out that they have been recorded without permission. Some states' anti-wiretapping statutes require consent of both sides of a telephone conversation for exactly this reason.[196] Regardless, the main problem with *White* was the perpetuation of the flawed rationale in *Hoffa* and *Lewis*.

C. *Privacy in Public*

One of the most commonly employed binaries for dismissing privacy concerns is the idea that there is no privacy in public.[197] *Katz* provides the germ of this principle: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[198] The Court has built a great deal of doctrine upon this idea. *United States v. Knotts*[199] is a prominent example:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [Defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[200]

In *Knotts*, both the Supreme Court and Court of Appeals agreed that there was no privacy in public, but the Supreme Court brushed aside the worries that a beeper *might* intrude on a private domain, noting that it had not actually done so.

> The Court of Appeals appears to have rested its decision on this ground:

---

195 *White*, 401 U.S. at 752.

196 *See, e.g.*, CAL. PENAL CODE §§ 631–32 (West 2012); MASS. GEN. LAWS ANN. ch. 272, § 99 (West 2012). These laws are not the only indication of the information flow disruption, and accordingly, the fact that not *all* states have two-way consent laws (or that several have carve-outs for law enforcement, see, for example, 18 PA. CONS. STAT. ANN. § 5704(2) (West 2012)) does not demonstrate a definitive lack of information flow disruption.

197 *See* NISSENBAUM, *supra* note 24, at 113.

198 Katz v. United States, 389 U.S. 347, 351 (1967).

199 460 U.S. 276 (1983).

200 *Id.* at 281–82. Other well-known examples are *California v. Ciraolo*, 476 U.S. 207 (1986), and *Florida v. Riley*, 488 U.S. 445 (1989), discussed earlier. *See supra* notes 69–72 and accompanying text.

> "[A] principal rationale for allowing warrantless tracking of beepers, particularly beepers in or on an auto, is that beepers are merely a more effective means of observing what is already public. But people pass daily from public to private spheres. When police agents track bugged personal property without first obtaining a warrant, they must do so at the risk that this enhanced surveillance, intrusive at best, might push fortuitously and unreasonably into the private sphere protected by the Fourth Amendment."
>
> We think that respondent's contentions, and the above quoted language from the opinion of the Court of Appeals, to some extent lose sight of the limited use which the government made of the signals from this particular beeper. As we have noted, nothing in this record indicates that the beeper signal was received or relied upon after it had indicated that the drum containing the chloroform had ended its automotive journey at rest on respondent's premises in rural Wisconsin.[201]

The private/public rationale is amplified in *United States v. Karo*,[202] a subsequent case presenting quite similar facts.[203] The operative difference between the two is that in *Karo*, unlike in *Knotts*, the police continued to track the person inside a home.[204] Based on that difference alone, the Court in *Karo* found a Fourth Amendment violation.[205] While it is certainly intuitive that a person has a right to expect *more* privacy in the home, these cases create a hard-line distinction. Moreover, these two cases ignore the observation from *Katz* that the Fourth Amendment "protects people, not places."[206]

Needless to say, these two cases are analyzed differently under contextual search doctrine. *Knotts* is a more complex case than the previous ones, with more information flows, so the analysis illuminates more about the theory's operation. The facts of *Knotts* are as follows: Minnesota police suspected that one co-defendant, Armstrong, would purchase chloroform as part of an illegal drug manufacturing operation.[207] The police then convinced the seller of the chloroform to

---

201 *Knotts*, 460 U.S. at 284–85 (quoting United States v. Knotts, 662 F.2d 515, 518 (8th Cir. 1981), *rev'd*, 460 U.S. 276 (1983)).

202 468 U.S. 705 (1984).

203 *Id.* at 707–11.

204 *Id.* at 714.

205 *Id.* ("This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. Contrary to the submission of the United States, we think that it does.").

206 Katz v. United States, 389 U.S. 347, 351 (1967). The home, however, is still worthy of protection as a social context, as well as a place. The rationale just needs to change, and with it, the hard line approach. *See infra* Part V.A.

207 *Knotts*, 460 U.S. at 278.

insert a "beeper" into one of the purchased containers.[208] In the words of the Court, "[a] beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."[209] The police used the beeper to follow Armstrong from the chemical company to the cabin of a second defendant and the respondent, Knotts.[210] Knotts then argued that the evidence found at his home should be suppressed as a fruit of an illegal search, specifically the use of the beeper to reveal the location and existence of his home.[211]

Knotts contains two important information flows and overlapping contexts. The problem can be simplified after examining the relationship between Armstrong and Knotts (and a third co-defendant), presumably that of friends or business partners. For the sake of simplicity, assume that Knotts and Armstrong had a typical information sharing relationship for business partners: open sharing with each other and each trusted the other to be judicious about further sharing. That is, if either Armstrong or Knotts started speaking about their activities and location broadly, or specifically to the police, it would have violated the transmission principle governing their relationship. Wherever control is a part of the transmission principle, it is reasonable to assume that Armstrong and Knotts would have chosen to exercise the same level of control over information, vis-à-vis outsiders, and thus they can be reduced to a single unit, referred to as the "defendant" for the rest of the analysis.

The two remaining information flows are 1) the police following the defendant; and 2) the chemical seller installing the beeper, which in turn broadcasts the defendant's whereabouts. The first concerns the relationship between defendant as subject and sender of his own whereabouts, and the police as receiver. The second concerns the police as receiver, the seller as sender (because he changed the information flow, making it available to the police), and the defendant as subject.

The transmission principle for the first information flow is not obvious. The reasons to be apprehensive about being followed by a stranger are different than those that might apply to being followed by the police. When a stranger follows someone, the subject is likely to be worried about the potential for physical harm, either present or at some later time. With the police, however, there is less of a worry that the police will be following someone for the purpose of an assault. Still, there is good reason to worry about police following someone in the

208 *Id.* This should immediately call to mind the informant cases, which we shall soon see are quite related to *Knotts* in ways the Court could not have explored given the shape of its jurisprudence.

209 *Id.* at 277.

210 *Id.* at 278.

211 *Id.* at 279.

absence of individualized suspicion, as without *any* suspicion it is probably for some illicit motive, such as improper profiling. We do expect police to (literally) follow leads when necessary, however. Thus, while a flat prohibition on police following cannot be the correct norm, it does not follow automatically that there should be *no* limits.[212] This error is laid plain by the holding of *Karo*, which held the police were not permitted to follow the defendant once he was inside a house.[213] So then the question is whether there is a binary distinction between "in public" and not, or whether there is a spectrum along which some following is permitted and more is not. The spectrum answer seems more intuitive[214]: the more intrusive the following, the higher level of suspicion and procedural protections that should be required.[215] This is at least part of the intuition behind the concern about prolonged surveillance in *Jones*.[216]

Lacking empirical data about society's views on permissible police conduct, the exact transmission principle is unclear. The violation inquiry will therefore be inconclusive. In *Knotts*, the beeper was used only in a limited capacity, and the Court specifically noted that there was neither twenty-four hour surveillance[217] nor continued use once defendant was inside a private home.[218] So, leaving aside the technology for the moment (the specific effects of technology are discussed in Part IV), this means that the officer followed the suspect without a warrant, but probably with some level of suspicion and for only a moderate length of time. Given these intermediate circumstances, it is impossible to say here whether the first information flow violated an informational norm.

The second information flow did violate a norm. The actors are identified above, the attribute of interest is still the defendant's whereabouts, and the relevant transmission principles are those governing the market context. Information necessary to complete the sale will flow freely between the seller and buyer, such as credit card information, address, phone number, and items purchased.[219] That

---

212 *Contra id.* at 281–82.

213 United States v. Karo, 468 U.S. 705, 716–18 (1984).

214 With any proportionality principle there will be concerns regarding administration. *See infra* notes 413–415 and accompanying text (discussing the proportionality principle).

215 Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012).

216 United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

217 *Knotts*, 460 U.S. at 283.

218 *Id.* at 284–85.

219 This is a case where two different contexts, one fully encompassing the other, might be appropriate. The relevant context here might be "the market for dangerous chemicals," rather than the larger market. Because certain chemicals are inherently dangerous, or perhaps because they are used to manufacture drugs, the chemical sale context might include a transmission principle allowing information to flow to the police if there is reason for suspicion. As

information was subject to an expectation of confidentiality.[220] With respect to the whereabouts of the customer after leaving the store, however, that information is in complete control of the customer. He may tell the storeowner he is going fishing right after leaving the store, but if he does not mention anything, the store owner may not follow him to the lake. The *control* principle, illustrated here, protects the customer's whereabouts from both the seller and any third party, such as the police, whom the seller might inform.

Now consider the violation inquiry. By inserting the beeper, the seller took the information out of the defendant's control and thus violated the norm, even though he did not have access to the information himself. Because the seller's violation was done at the behest of the police, it implicates the Fourth Amendment.

The normative analysis, then, needs to determine whether allowing the police to get a businessperson to change this information flow is preferred over the status quo. If people knew that a seller was more likely than others to cooperate with police, customers would take more precautions with purchases, and instead of competition being based on the quality of products or even brand loyalty, they would be based partially on likelihood of passing information to the police. Some might argue that this is something that *should* be priced into the market, but this seems like a descriptive claim that the market can solve the problem, rather than a normative claim that it should. If it is not normatively desirable within the market context, then the change must be balanced against the ability of the police to track suspects, and a

---

discussed earlier, the choice of context is a normative task that can be solved iteratively. *See supra* note 57 and accompanying text.

Before getting to the normative questions, though, the appropriate context can be narrowed to two reasonable possibilities, and a full analysis would use both possibilities. With respect to the particular information at issue—the defendant's *whereabouts*—the transmission principle is likely the same, so there is a shortcut here. The differences come when considering heavy regulation and the need to report typical transaction information to the authorities, but that information is not at issue here.

An alternative approach to this distinction would be to suggest that within the general market context, sales of certain dangerous items are subject to a different transmission principle. The effect appears to be the same, but whether one is preferable depends on how generally context should be defined. Contexts should continue to be useful social contexts to have any useful meaning, but the "too small to be useful" line is certainly fuzzy. *See* NISSENBAUM, *supra* note 24, at 223.

220 Due to e-commerce, this expectation has changed such that people are surely comfortable with some level of commercial information sharing, though when people are more aware of it, they will pay more for better privacy. *See* Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYSTEMS RES. 254 (2011). Nonetheless, withholding information from the police is still the norm. Dieter Bohn, *Google, Microsoft, Yahoo, and Facebook Say They Require Warrants to Give over Private Content*, THE VERGE (Jan. 26, 2013, 6:57 AM), http://www.theverge.com/2013/1/26/3917684/google-microsoft-yahoo-facebook-require-warrants-private-content.

warrant requirement slows that process. In the end, again, the answer is unknown.

Interestingly, under contextual search doctrine, similarities between *Knotts* and the informant cases become apparent, due to the use of a third party to redirect the information. Because the Court relied on the "no privacy on public roads" rationale, considering only the act of following,[221] the cases did not seem similar before. Considering context, it is clear now that the same normative arguments about whether society wants to condition banking, phone use, or social relationships on the waiver of privacy apply here to the market context, counseling against giving the police carte blanche to use third parties for tracking.

D. *Emanations*

Cases about emanations are substantively different than the cases discussed so far. All people continually emanate light, heat, smells, sounds, and other information,[222] including DNA.[223] These emanations contain a great deal of information about a person, and technology enables the police to glean ever more from these involuntary excretions. For the most part, search doctrine has not considered emanations as their own set of information, treating them differently depending on the case. For example, using dogs to sniff for drugs is not a search under current doctrine, except when used to search someone's home.[224] Dogs, the Court stated in *Illinois v. Caballes*,[225] are a sui generis case because they only give the limited information about whether or not illicit drugs are present.[226] On the other hand, the Court treated emanated heat very differently in *Kyllo v. United States*,[227] holding that the use of heat-sensing technology to observe information that "could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" was a search.[228] The fact that the heat emanated into public did not matter because the police used technology that was not

221 *Knotts*, 460 U.S. at 281–82.

222 Ian Kerr & Jena McGill, *Emanations, Snoop Dogs and Reasonable Expectations of Privacy*, 52 CRIM. L. Q. 392, 393 (2007).

223 Elizabeth E. Joh, Essay, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006); *see also* Maryland v. King, 133 S. Ct. 1958, 1963–64 (2013) (likening DNA to a fingerprint).

224 Florida v. Jardines, 133 S. Ct. 1409 (2013).

225 543 U.S. 405 (2005).

226 *Id.* at 409. In reality, drug dogs are unreliable, as Justice Souter pointed out in his *Caballes* dissent. *Id.* at 410 (Souter, J., dissenting). For the purpose of this discussion, however, this is not immediately relevant.

227 533 U.S. 27 (2001).

228 *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

generally available to the public to detect the emanation.[229] Just this year, these two holdings came into direct conflict in *Florida v. Jardines*,[230] a case about using trained dogs to detect drugs on the front porch of a person's home.[231] As this section demonstrates, Justice Kagan's concurrence is a perfect example of how contextual search doctrine treats emanations.[232]

Emanations can be described by information flows just like anything else. In people's day-to-day lives, they expect that others can see them walking around and can hear some level of what they do. People disguise themselves to avoid being recognized and lower their voices to avoid being overheard. These observations are at the heart of the Court's complaint that police need not "avert their eyes,"[233] and here the Court is absolutely right. With respect to emanations, however, the typical information flows rely on several other assumptions, such as practical obscurity. When pedestrians walk down the street, they do not expect to be recorded, except possibly by the passing tourist or artist, who has no interest in the subject and treats him as part of the scenery. People expect to be forgotten because each of us is irrelevant to most passersby. Customers in cafes have private conversations expecting that no other customers care what they are saying and thus will not retain it or connect it back to them. In the case that someone suspects otherwise—a celebrity, for example, or a person in a small, gossipy town—he or she will take greater care to protect the information.

Part of society's reasonable expectation is that information flows will be limited by human capabilities. Humans have a limited degree of perception. Speaking at normal volumes inside homes, they reasonably expect not to be overheard because humans cannot hear through the walls.[234] When the police listen in, either with their ear to the door or with a microphone, they are violating that expectation.[235] The same goes

229 *Id.* at 34–36.

230 133 S. Ct. 1409 (2013).

231 *Id.* at 1412.

232 *Id.* at 1418–20 (Kagan, J., concurring).

233 California v. Greenwood, 486 U.S. 35, 41 (1988).

234 This raises the worrisome question whether those that can only afford small apartments and thin walls would have lesser Fourth Amendment rights than those with houses. A full treatment of that question is beyond the scope of this Article, but it is at the least no less true of contextual search than current doctrine. Jordan C. Budd, *A Fourth Amendment for the Poor Alone: Subconstitutional Status and the Myth of the Inviolate Home*, 85 IND. L.J. 355 (2010); Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391 (2003). Moreover, it is possible that a clearer picture of privacy norms, focusing on social context, will enable further legal protections where the less privileged lack the protections of the "reasonable person" in a given social context such as the home.

235 Note that these two violations are different degrees of intrusion as well. The ear to the door is something anyone can do, but the microphone is not and is more intrusive. *See* Kyllo v. United States, 533 U.S. 27, 35–40 (2001) (discussing "through-the-wall surveillance" technology).

for smells. When people smoke marijuana, they generally understand that people nearby can smell it, and sometimes take precautions such as a wet towel under the door. If the police smell the marijuana, they would not be required to ignore their noses, but the "plain smell doctrine" does not justify employing a dog to smell what would otherwise go undetected.[236]

Sensory information is bounded in time as much as other limits of perception. Recording allows emanations to be witnessed long after they have passed, by people who may or may not have been present to witness them. Thus, photographs, and video or audio recordings are also information flow disruptions. Human memory is faulty, and juries feel differently about recordings than live testimony from witnesses.[237] This is not to say that capturing all emanations requires a warrant, but rather that the act of changing the information flows about emanations is what dictates whether the Fourth Amendment applies—in other words, exactly the same considerations as every other information flow.

In this light, *Caballes* and *Kyllo* were difficult to reconcile. In both cases, police take an action that goes beyond unwittingly noticing that a certain emanation has occurred. If the police in *Kyllo* accidentally felt the heat or observed snowmelt while walking by the house, the case would have ended in favor of the government.[238] The lack of technology would have been the determining factor as the Court decided the case,[239] but in the framework proposed here, whether the police were searching for information is enough. Technology is responsible for many of today's changing information flows, but rather than analyze the technology directly, or its general availability, as the *Kyllo* Court did, cases should analyze a technology's effect on information flows just as they would analyze the effect of a new law or police practice.[240]

---

236 *Jardines*, 133 S. Ct. at 1418 (Kagan, J., concurring) ("Like the binoculars, a drug-detection dog is a specialized device for discovering objects not in plain view (or plain smell)."); *see also* Irus Braverman, *Passing the Sniff Test: Police Dogs As Surveillance Technology*, 61 BUFF. L. REV. 81, 85 (2013) (relying on a science and technology studies (STS) scholarship-based definition of technology—that technology is defined by reference to its place in, and effect on, society—to argue that drug-sniffing dogs are technology "in every relevant sense of the term").

237 Recall this issue appearing additionally in the difference between an informant reporting to the police and wearing a wire. See the discussion of *United States v. White*, *supra* Part III.B.

238 *Kyllo*, 533 U.S. at 35 n.2 ("The dissent's repeated assertion that the thermal imaging did not obtain information regarding the interior of the home is simply inaccurate. A thermal imager reveals the relative heat of various rooms in the home. The dissent may not find that information particularly private or important, but there is no basis for saying it is not information regarding the interior of the home. The dissent's comparison of the thermal imaging to various circumstances in which outside observers might be able to perceive, without technology, the heat of the home—for example, by observing snowmelt on the roof—is quite irrelevant. The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." (citations omitted)).

239 *Id.* at 34.

240 *See infra* Part V.

This is precisely how Justice Kagan analyzed the situation in *Jardines*.[241] Like in *Jones*, the *Jardines* majority focused on the trespass element: because the dogs were on the property to search, the Fourth Amendment was breached.[242] Just like in *Jones*, the concurring Justices reached the same conclusion under the privacy regime. Justice Kagan specifically likened the dogs to other sense-enhancing forms of technology, such as binoculars, noting that they were both "super-sensitive instrument[s]" used to accomplish the same goal.[243]

Whether or not technology is involved, if police act to disrupt an information flow in an unexpected way, the action is a violation of the Fourth Amendment, under Justice Kagan's reasoning. What makes Justice Kagan's analysis more than a straightforward application of *Kyllo* is that in the past, binoculars have not been considered a technology that would have triggered such a violation.[244] Justice Kagan was actually reasoning that it was the *act* of peering into the home, taking away information that would have normally been contained, that causes the violation.[245] Justice Kagan, though she used different terminology, was reasoning about information flows.

While the Court now treats dog sniffs as a search in the home, *Caballes* is still good law outside the home.[246] Under contextual search doctrine, this cannot be correct because police use dogs to change information flows intentionally. Instead (assuming drug dogs are reliable),[247] the Court's reasoning that they are less intrusive and only detect drugs[248] has merit for the *degree* of suspicion required. Perhaps instead of a warrant, police only need reasonable suspicion because the

241 133 S. Ct. 1409 (2013).

242 *Id.* at 1417 ("[W]e need not decide whether the officers' investigation of Jardines' home violated his expectation of privacy under Katz. . . . That the officers learned what they learned only by physically intruding on Jardines' property to gather evidence is enough to establish that a search occurred."). Interestingly, even Justice Scalia's majority opinion included a nod toward contextual social norms. *Id.* at 1416 ("To find a visitor knocking on the door is routine (even if sometimes unwelcome); to spot that same visitor exploring the front path with a metal detector, or marching his bloodhound into the garden before saying hello and asking permission, would inspire most of us to—well, call the police. . . . Here, the background social norms that invite a visitor to the front door do not invite him there to conduct a search.").

243 *Id.* at 1418 (Kagan, J., concurring).

244 Binoculars are clearly in general public use, and open windows of a home means that the home need not be physically invaded. *See* Minnesota v. Carter, 525 U.S. 83, 104 (1998) (Breyer, J., concurring). *Contra Kyllo*, 533 U.S. at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained . . . constitutes a search—at least where (as here) the technology in question is not in general public use." (citation omitted)).

245 *Jardines*, 133 S. Ct. at 1418 (Kagan, J., concurring).

246 *Id.* at 1417–18.

247 They are, however, likely not reliable. *See* Lisa Lit, Julie B. Schweitzer & Anita M. Oberbauer, *Handler Beliefs Affect Scent Detection Dog Outcomes*, 14 ANIMAL COGNITION 387 (2011).

248 Illinois v. Caballes, 543 U.S. 405, 409 (2005).

search is less intrusive than a full search. A reasonable suspicion requirement would still avoid the current doctrine's problem of allowing police to bring drug dogs indiscriminately into every encounter with a car, even among DUI stops or parked cars.[249] The same analysis applies to thermal imagers: the limited quantity of information goes to the degree of suspicion required to use them, not whether or not *any* suspicion is required. By refusing to call a drug sniff a search, or by limiting consideration of technology to that which is not in common use, the Court unnecessarily removes the possibility of debate about the correct level of suspicion or oversight.[250] Hopefully, Justice Kagan's concurrence is the beginning of a trend in the Court's treatment of emanations.

E. *Roving Wiretaps*

The analysis so far has largely focused on areas in which the doctrine does not adequately respect context. Not everything becomes more difficult for police when the focus shifts to social context. Roving wiretaps, for example, are more easily justified under a contextual regime. Roving wiretaps are wiretaps that have a person as a target, rather than a specific phone number.[251] Traditional wiretaps require a new authorization for each new phone number to monitor.[252] Roving wiretaps allow for a police officer to follow a particular *person*, as long as that person has been shown to use tactics to evade traditional wiretaps,[253] such as switching phones. Roving wiretaps were authorized federally in the Electronic Communications Privacy Act,[254] which updated Title III of the Omnibus Crime and Control and Safe Streets Act of 1968 to include them, after it became clear that criminals were evading traditional wiretaps by changing cell phones.[255]

The Supreme Court has not weighed in on the constitutionality of roving wiretaps, but all the circuit courts to consider the issue have found them constitutional.[256] Each of these cases has found that the

---

249 *Id.* at 422 (Ginsburg, J., dissenting) ("Today's decision, in contrast, clears the way for suspicionless, dog-accompanied drug sweeps of parked cars along sidewalks and in parking lots.").

250 *See infra* notes 408–412 and accompanying text (discussing the proportionality principle).

251 18 U.S.C. § 2518(11)(b)(ii) (2012).

252 *Id.* § 2518(1)(b).

253 *Id.* § 2518(11)(b)(ii).

254 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

255 Bryan R. Faller, Note, *The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better*, 60 OHIO ST. L.J. 2093, 2098–100 (1999).

256 *See, e.g.*, United States v. Wilson, 237 F.3d 827, 831 (7th Cir. 2001); United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996); United States v. Bianco, 998 F.2d 1112, 1124 (2d Cir. 1993), *abrogated as noted by* United States v. Galpin, 720 F.3d 436 (2d Cir. 2012).

particularity requirement for a "place to be searched" was satisfied by the abstract concept of the place in which the suspect was speaking.[257] This seems like a twist of logic, but in truth, the concept of "searching" an audio track is inherently divorced from location anyway. Thinking about roving wiretaps in a social context makes them an easier case though. The point of a wiretap is not that a particular telephone line is being used to commit crimes, but that the person who happens to regularly use that line may be committing them.[258] Currently, an application for a roving wiretap has to show that the target has tried to evade traditional wiretaps.[259] Under contextual search doctrine, all wiretaps should be roving because it is a person that is the target, not a place. Once the warrant is obtained, the law enforcement context is most salient, and it is expected that phone communications will flow to the police, even as the suspect interacts with other contexts.

IV. TECHNOLOGY AND THE FUTURE OF SEARCH

The future of search doctrine lies in technology. New technology continually disrupts information flows, whether by capturing, recording, and processing more information than ever before, encouraging people to share personal information, or tethering people to a communication infrastructure that saves a history of locations and browsing habits. The most important thing to recognize in analyzing technology is that it is, in a sense, not special. Technology disrupts information flows in exactly the same ways that new laws or new police practices can, and the privacy backlashes in the news are usually not solely caused by the technology, but by its combination with a new policy.

For example, Facebook as a technology has changed information flows drastically, allowing people to share widely, but when analyzing the emerging trend of employers asking for Facebook passwords,[260] the technology is just one factor alongside the policy itself and the cultural trend of sharing. Similarly, GPS has disrupted information flows regarding location, but the Federal Bureau of Investigation's decisions about how to deploy GPS trackers are just as important as the technology itself in determining whether there is a violation of informational norms. Technology is intimately intertwined with the

257 *See, e.g.*, *Wilson*, 237 F.3d at 831; *Gaytan*, 74 F.3d at 553; *Bianco*, 998 F.2d at 1124.

258 *See, e.g.*, United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992).

259 *See* 18 U.S.C. § 2518(11)(a) (2012).

260 Michael Santo, *List of Employers Demanding Facebook Passwords Continues to Grow*, EXAMINER.COM (Apr. 2, 2012), http://www.examiner.com/technology-in-national/list-of-employers-demanding-facebook-passwords-continues-to-grow.

social context in which it is created or used.[261] Accordingly, just like any other information flow disruption, technology can and should be analyzed by how it disrupts those flows, regardless of the fact that it is "technology."

Search doctrine has encountered technology in several cases discussed earlier—*Knotts*, *Kyllo*, and *Jones* being the most prominent.[262] The discussion of technology in these cases focuses partly on the technology qua technology and partly on its effects. In *Knotts*, the Court suggested that the beeper only allowed police to observe what they otherwise could by the naked eye, and thus the technology was unimportant to the decision.[263] This conclusion could be supported by a contextual analysis too, saying that the information flows due to the technology did not change much from the standard situation of police following a subject; thus the rules of a physical following situation would apply.[264] The difference between approaches in this case is minimal because the reason for the dismissal of the technology is essentially its low impact on information flows.[265]

Kyllo similarly gets it right, at least as applied to its own facts. The use of the heat-sensing technology allowed an officer to see what could not otherwise be seen without intrusion into the home and, therefore, it was ruled a search.[266] This is as close to contextual analysis as the Court gets. Normal eyesight cannot detect the heat patterns in this way, so irrespective of the fact that the heat is emanating, the police need to use a tool (and take deliberate action) to find out that marijuana is being grown in the house.[267] The Court then added that once such a technology is in general use by the public, there is no expectation of privacy.[268] If the Court were analyzing information flows rather than technology, this part of the opinion would not have been written. If the technology were publicly available and the general, socially acceptable public use was the same as the police use, then the use would be acceptable because it did not contravene entrenched informational norms.[269] However, reasoning about the availability of the technology

---

261 *See generally* Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 121 (1980).

262 *See supra* text accompanying notes 95, 218, 227–228.

263 United States v. Knotts, 460 U.S. 276, 282 (1983).

264 *See supra* Part III.B. This is not necessarily the proper conclusion, only a possible one. That police can "see" around corners and more easily avoid detection matters. *See* NISSENBAUM, *supra* note 24, at 145, 192 (discussing reciprocity).

265 *Knotts*, 460 U.S. at 282 ("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.").

266 Kyllo v. United States, 533 U.S. 27, 34 (2001).

267 *See id.* at 35 & n.2.

268 *Id.* at 34.

269 Note that even in this case, there is no guarantee that the transmission principles would be the same for the average citizen as for police.

without further examination into the resulting typical or appropriate information flows gets it wrong. What matters is not the technology, but the informational norms, even where the availability of technology itself has coincided with or even caused a change in those norms.

Finally, in *Jones*, the majority opinion relied on a trespass rationale: because the police attached a device to the underside of the car, a violation occurred.[270] Both Justice Alito's and Justice Sotomayor's concurrences, which analyzed the case under a more classic reasonable expectation of privacy rationale, focused on the effects of the technology: the information flows. Justice Alito called the use of GPS a "technique," and in evaluating the violation, he made no reference to the specific technology, but rather wrote, "I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[271] Justice Sotomayor likewise stated:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[272]

This treatment of technology is fundamentally correct. As commentators were quick to point out, though, the concurrences lacked a test or framework[273] for determining exactly what qualifies as "longer term GPS monitoring" subject to the Fourth Amendment.[274] In order for law to respond to changing technology and avoid obsolescence, it must be technology-independent, focusing only on information flows. Such a treatment obviates the need to answer the question with respect to a specific technology, but does require that the question be answered generally. Because the Court has already addressed GPS, this Part examines a few other technologies increasingly commonly used by law enforcement—cell phone location data;[275] visual surveillance and

---

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

271 *Id.* at 957–58 (Alito, J., concurring).

272 *Id.* at 956 (Sotomayor, J., concurring).

273 *E.g.*, Goldstein, *supra* note 7; Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431, 431–32 (2013); *see also* Jim Harper, U.S. v. Jones: *Fourth Amendment Law at a Crossroads*, CATO INST. (Sept./Oct. 2012), http://www.cato.org/policy-report/septemberoctober-2012/us-v-jones-fourth-amendment-law-crossroads.

274 *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

275 Eric Lichtblau, *Police Are Using Phone Tracking As Routine Tool*, N.Y. TIMES, Apr. 1, 2012, at A1.

recording, such as automatic license plate recognition (ALPR);[276] surveillance cameras[277] and drones;[278] and social networks[279]—and discusses how they can be treated focusing on information flows. One noteworthy aspect is the similarities to prior cases that arise from this type of consideration.

A. *Cell Phone Location Data*

Cell phone location data offers a more complete picture of a person's whereabouts than GPS.[280] The GPS tracker in *Jones* had to be installed on a person's car,[281] but phones automatically track location for the purposes of providing service, just by virtue of being turned on.[282] Additionally, people carry their phones with them at all times of day, even routinely sleeping with their phones on their nightstands.[283]

Police routinely use cell phone location data to track people.[284] Cell phone location data is collected by the carriers as mandated both by

---

276 Mary Beth Sheridan, *License Plate Readers to be Used in D.C. Area*, WASH. POST BREAKING NEWS BLOG (Aug. 17, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/16/AR2008081602218.html.

277 Spencer S. Hsu, *D.C. Forms Network of Surveillance: Police Video Links Raise Rights Issues*, WASH. POST, Feb. 17, 2002, at C1.

278 Brian Bennett, *Spy Drones Aiding Police; The Use of Predators in Pursuing Crime at Home Troubles Privacy Advocates.*, L.A. TIMES, Dec. 11, 2011, at A1.

279 *See* Seth Augenstein, *Police on Facebook: Law Enforcement Using Social Media to Connect with Public*, THE STAR LEDGER (Sept. 1, 2013), http://www.nj.com/sussex-county/index. ssf/2013/09/to_like_leads_and_share_tips_facebook_police_pages_help_investigation_prompt_debate.html; Kate Knibbs, *In the Online Hunt for Criminals, Social Media Is the Ultimate Snitch*, DIGITAL TRENDS (July 13, 2013), http://www.digitaltrends.com/social-media/the-new-inside-source-for-police-forces-social-networks.

280 AM. CIVIL LIBERTIES UNION, ACLU AFFILIATE NATIONWIDE CELL PHONE TRACKING PUBLIC RECORDS REQUESTS: FINDINGS AND ANALYSIS (2012), *available at* https://www.aclu.org/files/assets/cell_phone_tracking_documents_-_final.pdf; Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker.*, N.Y. TIMES (July 15, 2012), http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html.

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

282 Maass & Rajagopalan, *supra* note 280.

283 Douglas McIntyre, *Do You Sleep with Your Cell Phone? Most Americans Do*, DAILYFINANCE (Sept. 3, 2010, 6:04 PM), http://www.dailyfinance.com/2010/09/03/do-you-sleep-with-your-cell-phone-most-americans-do-study-find.

284 The *New York Times* ran a front page story about local police departments' use of this practice, which might be more surprising than hearing the FBI is doing the same. Lichtblau, *supra* note 275. The practice is so common that in Antoine Jones's retrial (necessitated by the Supreme Court's remand in *Jones* several years after the investigation), the prosecutors revealed that they also had five months of cell site location data on which to base their case. David Kravets, *After Car-Tracking Smackdown, Feds Turn to Warrantless Phone Tracking*, WIRED (Mar. 31, 2012), http://www.wired.com/threatlevel/2012/03/feds-move-to-cell-site-data. A particularly damning quote in the *Times* article, from the Iowa City Police Department training manual, demonstrates an awareness that this practice violates privacy: "'Do not mention to the public or the media the use of cellphone technology or equipment used to locate the targeted subject.'" Lichtblau, *supra* note 275. The training manual also advised the tracking "be kept out

pure functionality and by law for emergency services.[285] Cell phone carriers then keep this data for a long time, usually a year or more.[286] This storage may or may not be justified,[287] but the information flow relevant to the Fourth Amendment is not the storage, but rather the downstream one in which the police (the receiver) obtain the data from the carrier (the sender) about the customer (the subject).[288] The trick here is to identify the transmission principle.

Given the speed with which norms change in the use of technology, identifying specific transmission principles is nearly impossible. It is easier to determine what is clearly prohibited. To the extent the data collection is justified, it would be for limited, expected uses: serving local ads, using mapping or restaurant recommendation apps, or other related uses. It is implausible, however, to argue that the great number of people who do not even recognize that the phone company collects this data would find its transmission to the police appropriate without a warrant.[289] A rule by which the police could obtain this data simply by virtue of its existence would mirror the *Miller* rule in the banking context, essentially conditioning all cell phone use on a waiver of Fourth Amendment rights.[290] Such a rule would be even more troubling than in the banking context because cell phone history is often more revealing than bank accounts.[291] Police use of cell phone location data is actually making its way through the courts now,[292] and at least one court has

---

of police reports." *Id.* The expected outrage is, as always, good evidence that the practice would violate informational norms.

285 Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (1994).

286 Darlene Storm, *How Long Does Your Mobile Phone Provider Store Data for Law Enforcement Access?*, COMPUTERWORLD (Sept. 28, 2011, 5:09 PM), http://blogs.computerworld.com/19016/how_long_does_your_mobile_phone_provider_store_data_for_law_enforcement_access.

287 It is not clear whether this collection and storage itself violates informational norms. Many people are not aware of the data collection and storage, so it is possible that whatever norm a hypothetical public that is educated about the data storage would have would not allow this, and it is hard to discuss a norm about a practice that is mostly unknown. However, when police access the information, it is a further disruption in flow that can be analyzed separately. For these purposes, we can assume the carriers' collection and storage is permissible and analyze just the law enforcement involvement.

288 AM. CIVIL LIBERTIES UNION, *supra* note 280, at 5.

289 New Jersey v. Earls, 70 A.3d 630, 643 (N.J. 2013) ("People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with the police.").

290 *Cf.* United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.").

291 Maass & Rajagopalan, *supra* note 280.

292 *In re* United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that because use of cell phones was voluntary, collecting cell site data falls under the third-party

demonstrated that reasoning about expected information flows and separating predictive "expectation[s]" from "legitimate privacy interest[s]" is a feasible approach.[293]

B. *Pervasive Visual Surveillance and Recording*

Several of the technologies growing in popularity have similar effects on information flows. Automatic License Plate Recognition (ALPR) systems read and record license plates of cars that pass their cameras.[294] Ubiquitous surveillance cameras capture and store full streams of their entire visual fields,[295] and drones do the same while flying around, only at greater capacity and resolution.[296] Combined with advancing facial recognition technology,[297] the visual surveillance from stationary and drone-mounted cameras has a potential for automation and searchability, while the ALPR system already contains those attributes.[298]

Each of these technologies can be as invasive as cell site information. In Washington, D.C., for example, there is reportedly more than one license plate reader per square mile.[299] Some are stationary, and others are mounted on patrol cars, with the eventual goal being to have every police car equipped with a reader.[300] The cameras capture 1800 images per minute and are more than capable of capturing every license plate that drives by.[301] The police collect the license plates indiscriminately and hold them for a few years, hoping

---

doctrine and does not require a warrant); *Earls*, 70 A.3d at 641–42, 644 (holding that cell site data requires a warrant under the New Jersey constitution, though acknowledging that New Jersey does not follow the third-party doctrine).

293 *Earls*, 70 A.3d at 642–44.

294 *See generally* AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS (2013), *available at* http://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

295 *Id.* at 4.

296 *See, e.g.*, Liz Klimas, *Worried? New Drone-Mounted Camera Can Tell What You're Wearing from 17,500 Feet*, THE BLAZE (Jan. 29, 2013, 9:57 AM), http://www.theblaze.com/stories/2013/01/29/worried-new-drone-mounted-camera-can-tell-what-youre-wearing-from-17500-feet.

297 John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 81 (2002).

298 AM. CIVIL LIBERTIES UNION, *supra* note 294, at 4–5.

299 Liz Klimas, *Do D.C. Police License Plate Readers Lead to a 'Surveillance Society'?*, THE BLAZE (Nov. 26, 2011, 6:31 AM), http://www.theblaze.com/stories/do-d-c-police-license-plate-readers-lead-to-a-surveillance-society.

300 *Id.*; *see also* POLICE EXEC. RESEARCH FORUM, HOW ARE INNOVATIONS IN TECHNOLOGIES TRANSFORMING POLICING? iii, 2 (2012), *available at* http://policeforum.org/library/critical-issues-in-policing-series/Technology_web2.pdf (reporting that on average, agencies responding to the survey predict that by 2017, 25% of patrol cars will be equipped with ALPR technology).

301 Kilmas, *supra* note 299.

that one day the information will be useful.[302] A 2011 report found that 85% of police departments around the country plan to begin or increase use of ALPR in the next five years.[303]

In New York, there is an extremely high density of surveillance cameras.[304] In 2005, the New York Civil Liberties Union found 4,468 cameras viewable from street level below 14th Street alone, about five times the number they found in a similar study in 1998, in an area of about five square miles in Manhattan.[305] The density of placement in these two systems is important to understanding the granularity of the information. A single surveillance camera in a store is not intrusive for its customers, as it does not paint a total picture of the customer's life the way an entire network of cameras does.

Drone mounted cameras are not yet as widely used, but they have impressive surveillance power between their mobility, imperceptibility, and extreme range and resolution, and they are gaining popularity among police departments.[306] The domestic use of drones has increased in large part due to their success abroad,[307] and thus we should not be surprised when successful military technology becomes the next model of domestic drone as well. Other drones being developed are the size of birds or even insects.[308] The drones' capability to surveil an entire population in plain sight without possibility of detection is only hampered by their relative expense and later adoption.

In future search litigation, there might be a temptation to examine these technologies, realize that a line *somewhere* was crossed, and to try to simply limit the *amount* of surveillance. The debate has already begun

---

302 *See id.* ("'It never stops,' said Capt. Kevin Reardon, who runs Arlington County's plate reader program. 'It just gobbles up tag information. One of the big questions is, what do we do with the information?'").

303 POLICE EXEC. RESEARCH FORUM, *supra* note 300, at 2.

304 N.Y. CIVIL LIBERTIES UNION, WHO'S WATCHING? VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT 2 (2006), *available at* http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf.

305 Manhattan's total area is 23.7 square miles. *NYC Statistics*, NYCGO.COM, http://www.nycgo.com/articles/nyc-statistics-page (last visited Sept. 1, 2013). Additionally, these were only the cameras visible from street level. It is a very good bet that there were easily as many again hidden from view, and that the number has increased significantly in the last seven years.

306 *See* Jennifer Lynch, *FAA Releases New Drone List—Is Your Town on the Map?*, ELECTRONIC FRONTIER FOUND. (Feb. 7, 2013), https://www.eff.org/deeplinks/2013/02/faa-releases-new-list-drone-authorizations-your-local-law-enforcement-agency-map.

307 Larry Copeland, *Police Turn to Drones for Domestic Surveillance*, USA TODAY (Jan. 14 2011, 10:17 AM), http://www.usatoday.com/tech/news/surveillance/2011-01-13-drones_N.htm; Glenn Greenwald, *The Growing Menace of Domestic Drones*, SALON (Dec. 12, 2011, 11:58 AM), http://www.salon.com/2011/12/12/the_growing_menace_of_domestic_drones.

308 Elisabeth Bumiller & Thom Shanker, *War Evolves with Drones, Some Tiny as Bugs*, N.Y. TIMES, June 20, 2011, at A1.

to move toward the merits of "mosaic theory,"[309] which asserts that the composite picture is greater than the sum of its parts and thus total quantities of surveillance should be limited.[310] This is not the best way to analyze the problem.

Contextual analysis of these technologies requires an examination of each of their information flows, specific to each type of information gleaned. While ALPR systems primarily record license plate numbers,[311] surveillance camera and drone flows contain several attributes, from physical whereabouts, to clothing choices, to a person's associations—anything that could come from tracking a person on camera across time and space. While it is invariably true that the whole is greater than the sum, an analysis need not jump to the *whole* whole, as mosaic theory would.[312]

Users of all three technologies seek to alter information flows in three similar ways: by 1) making a large number of visual observations in otherwise "public" spaces, 2) recording and storing them, and 3) employing an automated search function within the databases of faces or license plate numbers that the technology accumulates. In each of these flows, the subject and unwitting sender is the target of the surveillance and the receivers are the police. The variety in attributes complicates the transmission principles, and the lack of analogue to this kind of capture of emanated images makes the specific results hard to predict, but it is probably safe to say that control would be an element.

Step One, the visual observations, immediately calls to mind the *Knotts* "privacy in public" rationale. Unlike GPS and cell site data, all three of these technologies actually use visual observation that could initially have been made by a police officer without much enhancement. At this step, the problem comes when considering that the coverage is extensive enough that no human-based system could ever match it, and expectations about what is public on the street rely on reciprocity.[313] One of the unanalyzed problems with *Knotts* was that it extended the ability of police to follow *absent detection*. These technologies, at least with respect to Step One, are extreme expansions of the *Knotts* beeper.

Step Two, the recording, is problematic in the same way as recording any emanations or conversations is.[314] Systematic recording

309 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (critiquing mosaic theory as a valid approach); Slobogin, *supra* note 215 (proposing a mosaic theory legislation).

310 Kerr, *supra* note 309, at 320.

311 *But see* AM. CIVIL LIBERTIES UNION, *supra* note 294, at 6 & n.17 ("Photographs captured by license plate readers may contain more than simply the license plate.").

312 For ALPR, mosaic theory and the contextual analysis would be similar, as location is really the only information type being transferred.

313 *See* NISSENBAUM, *supra* note 24, at 145, 192.

314 *See supra* Parts III.B, III.D.

changes the flow of "public" observations from what people expect from their knowledge of the limits of human perception and memory. Additionally, by recording at one point and analyzing later, the devices can capture information faster than a human, and thus capture *more* information. It is impossible to imagine, for instance, the police officer capable of cataloguing 1,800 license plate numbers per minute without filming and then watching later. Finally, the availability of historical information raises the same problems that it does in cell site tracking: the information captured by these technologies would not have been captured by physical surveillance because the police would have had no reason to be watching.[315]

Step Three, the database search, turns what would otherwise be an unmanageable pile of individual images and numbers into useful information. Due to technological feasibility, searching is much more prevalent in ALPR than the photo databases. Facial recognition is much more challenging than capturing and digitizing license plate numbers because of the high degree of variability in faces and background conditions, but the technical capability will come.[316] In all these cases, the ability to search after the fact makes indiscriminate collection of data useful in the first place and untethers data collection from resource limitations. There is no analogue in people's privacy expectations for this step, because searchability of a database is never important until

---

315 The ACLU of New Jersey's brief in *Earls* discussed this with respect to cell site information:

> When police seek historical location information, they may retrospectively obtain data for times when physical surveillance was never done or even contemplated. For example, were police investigating a months-old crime, historical location information could trace a suspect's movements around the time of the crime. Police would not have surveilled at the time because the crime had not yet occurred.

Brief for The American Civil Liberties Union of New Jersey Foundation and The Association of Criminal Defense Lawyers of New Jersey as Amici Curiae Supporting Appellant at 33, New Jersey v. Earls, 70 A.3d 630 (2013) (No. A-53-11 (068765)), *available at* http://epic.org/amicus/location/earls/ACLUNJ-Earls-Amicus-Brief.pdf.

316 LUCAS D. INTRONA & HELEN NISSENBAUM, N.Y. UNIV. CTR. FOR CATASTROPHE PREPAREDNESS & RESPONSE, FACIAL RECOGNITION TECHNOLOGY: A SURVEY OF POLICY AND IMPLEMENTATION ISSUES (2009), *available at* http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf. Facebook is beginning to solve two different problems with facial recognition. First, it is providing contextual information, such as residential location and social networks of associates, that help narrow the field of possible facial matches enough that off-the-shelf facial recognition software may accomplish searchability. Alessandro Acquisti, Ralph Gross & Fred Stutzman, *Faces of Facebook: Privacy in the Age of Augmented Reality*, Presentation at Black Hat Technical Security Conference: USA 2011 (Aug. 4, 2011), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf. Second, Facebook provides a facial database to match a face with a name. Facial recognition was previously limited mainly to criminal databases for this reason. *See, e.g.*, Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571. Eventually, it is easy to imagine that facial identification could simply become a matter of access to Facebook's database and enough computing power.

there is more data than current privacy expectations would likely permit.

The information flows created by these technologies represent departures from the in-person police surveillance and investigation techniques that make up society's common understanding of police work. Each of the three steps described potentially violates informational norms. As norms change to adapt to technology, however, the first two may be less problematic. Mobile phones are ubiquitous, and indiscriminate recording is becoming more common. By analyzing the information flows, rather than just the quantity of information collected, it is possible to discuss the different points within the flows where the privacy harms are caused, and respond with targeted solutions. While the three-step flow as a whole is harmful, each individual change may not be, standing alone. *Collecting* the information may soon be considered acceptable, for example, as it becomes more commonplace, but a warrant requirement to search the resulting database could still interrupt the undesired information flows until there is a judicial determination of probable cause.

C. *Online Social Networks*

Social media, such as Facebook and Twitter, are another wealth of information for police. Police can easily scan any information that is unprotected by any privacy settings. Legally, this information is governed by the plain view doctrine.[317] Beyond unprotected information, describing the expected information flows on Facebook is incredibly difficult. If a user limits a post to her own friends, the user expects her friends to be able to see it.[318] She is relying on informational norms in the "friendship" context to curb future dissemination.[319] Her friends should know whether the shared information is sensitive and to what degree.[320] These considerations are more relaxed for a Facebook post than a one-to-one communication between friends because it is a form of broadcast, but teenagers, for example, still care if information on Facebook gets back to their parents or teachers.[321]

---

317 Though under this theory, the act of searching for this information online is legally a "search." *See supra* Parts II.B–C.

318 *See Choose Who You Share With: How Privacy Works When You Share*, FACEBOOK, http://www.facebook.com/help/445588775451827#!/help/459934584459934 (last visited Oct. 9, 2013) [hereinafter *How Privacy Works*].

319 *See* Alice E. Marwick & danah boyd, *I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience*, 13 NEW MEDIA & SOC. 114, 116 (2011).

320 *See How Privacy Works*, *supra* note 318.

321 Alice E. Marwick et al., *Youth, Privacy and Reputation (Literature Review)* 65 (Harvard Law Sch., Harvard Pub. Law Working Paper No. 10-29, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163.

If a user instead allows "friends of friends" to see a post, it is more public, but less so than a fully public post; it does not, for example, come up in open search results.[322] There is less expectation that a user has control over a "friends of friends" post, because there is little to no control over who exists at the second level of the network.[323] Importantly, evidence suggests that many users of Facebook do not understand how their privacy settings work in practice.[324]

Users' lack of knowledge about how information is actually flowing makes it very difficult to discern the informational norms. Without knowing the rules of this particular social context, a contextual analysis is difficult. In part, the norms must be similar to the familiar contexts in society, especially where people have the option of disaggregating groups into "circles"[325] or "lists"[326] of acquaintances, colleagues, family, or friends. But the ability to communicate with all of your friends at the same time is new, and few people do disaggregate lists, leading to a "collapse of contexts," as information is broadcast indiscriminately between social groups.[327] For "public" information, the police are taking an action to search Facebook, though there is a good argument the search is reasonable.

More interestingly, police have set up fake social media accounts in attempts to track some criminal suspects—a practice sure to gain currency in the future.[328] As far as police-owned fake profiles, the

---

322 *See Choose Who You Share With: Your Audience Options*, FACEBOOK, https://www.facebook.com/help/459934584025324 (last visited Oct. 9, 2013) (comparing "Public" with "Friends of Friends" settings).

323 Lior Strahilevitz has proposed an offline "social network" theory of privacy, based on practical analyses of information flow in social networks. He suggests a reasonable expectation of privacy at the "friend of friend" level, but not beyond. Strahilevitz, *supra* note 28, at 967–68.

324 Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. COMPUTER-MEDIATED COMM. 83, 94 (2009) ("[W]hile the majority of respondents claim to understand Facebook's privacy settings and restrict their profiles, the minority who report being unfamiliar with the privacy settings are not restricting their profile. Additionally, the descriptives of respondents' actions speak differently: Extensive personal information is being uploaded and protected with suboptimal access restrictions, in effect making it accessible to large groups of people that the respondent may not personally know—which further illuminates the fact that participants may indeed have a limited understanding of privacy issues in social network services.").

325 Anson Alexander, *Guide to Working with Circles in Google Plus [Google+]*, ANSONALEX.COM (July 2, 2011), http://ansonalex.com/tutorials/managing-circles-in-google-plus.

326 *How Do I Use Lists to Organize My Friends?*, FACEBOOK, https://www.facebook.com/help/?faq=200538509990389 (last visited Sept. 1, 2013).

327 Marwick & Boyd, *supra* note 319.

328 *Police Befriend Facebook, Twitter Users*, CBC NEWS (Oct. 7, 2009, 4:05 PM), http://www.cbc.ca/news/canada/ottawa/story/2009/10/07/ottawa-police-facebook-twitter-social-media.html; Dan Solomon, *Police Use Fake Facebook Profile to Bust Underage Drinkers—Is It Legal?*, ASYLUM (Dec. 4, 2009), http://www.asylum.com/2009/12/04/fake-facebook-profile-helps-police-bust-underage-drinkers-is.

analysis of the pretend friend cases is probably the most similar.[329] However, while a user that adds the police officer himself might be said to assume the risk (if the outcome of the cases were accepting as they stand today), the rationale is even harder to apply to the "friends of friends" posts two degrees removed from the officer. Counter to that, though, is the understanding that "friends of friends" posts are much more public than friends only.[330] While the informational norms here are not well understood, thinking about the information flows this way can at least inform the proper questions to ask about police in social networks.

V. PUTTING CONTEXT IN CONTEXT

The bulk of this Article has focused on using context to change the look of Fourth Amendment doctrine. This last Part, on the other hand, discusses a few parts of the Fourth Amendment that are already context-conscious, though mostly in hidden ways. A consideration of context is actually written directly into the text of the Fourth Amendment: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*."[331] Every part of the doctrine has scope limitations that restrict a search to its proper context—from warrants[332] and searches incident to arrest,[333] to automobile searches,[334] and administrative searches.[335] For a warrant to be valid, the place to be searched and things or people to be seized must be specified and related to the crime for which the warrant is issued to investigate.[336] This inherent contextual limitation is the direct consequence of free society's disdain for general warrants.[337] Awareness of context has always been central to the prevention of arbitrary use of police power, and thus, many of the rulings outside search doctrine align nicely with contextual integrity. As this Part demonstrates, contextual considerations go beyond search and can actually be a unifying principle to understand the broader Fourth Amendment.

---

329 *See supra* Part III.B.

330 *See How Privacy Works*, *supra* note 318, at *Can People See Who I'm Sharing With?*.

331 U.S. CONST. amend. IV (emphasis added).

332 *Id.*

333 Chimel v. California, 395 U.S. 752 (1969).

334 Arizona v. Gant, 556 U.S. 332 (2009).

335 New Jersey v. T.L.O., 469 U.S. 325, 357 (Brennan, J., concurring) (permitting administrative search "[o]nly where the governmental interests at stake exceed those implicated in any ordinary law enforcement context").

336 KAMISAR ET AL., *supra* note 121, at 305–08.

337 Amsterdam, *supra* note 103, at 411.

A. *Scope Limitations and Spatiotemporal Context*

Students are taught on the first day of criminal procedure that everything in the Fourth Amendment has scope limitations.[338] Scope limitations function as partial transmission principles: they prescribe limits on the flow of information. Thus, discussions of scope in the various cases follow closely with what contextual integrity would predict. When a warrant exception allows a search, a litigant who wants to extend the exception argues that the context is similar in the two cases. A litigant who wants to create a new exception will argue instead on normative grounds: the evidence is easily destructible, officer safety requires a new exception, or something else acts as a trump card. That is, the argument parallels the normative layer of contextual integrity, recognizing a prima facie violation but arguing for a new rule.

Consider the "search incident to arrest" warrant exception. The modern version of the exception, derived from *Chimel v. California*,[339] permits the police to search the area "within [the arrestee's] immediate control," and not other rooms in the premises or closed drawers the arrestee cannot reach.[340] According to the Court, danger to the police or possible destruction of evidence are the justifications, so the exception must be limited to the physical area in which those are valid concerns—the area of immediate control.[341] In a contextual analysis, the normative layer would have concluded that these rationales are acceptable, as long as they are limited as narrowly as possible, just as the Court did. In a later case, the Court extended the doctrine to provide for a "protective sweep," based on a reasonable suspicion of an assailant hiding in a closet or another room, but again, limited the sweep only to the areas representing a legitimate danger.[342] Under contextual analysis, given the existence of the prior normative result, it is not clear that this extension would even have caused a prima facie violation. The transmission

---

338 *See* Horton v. California, 496 U.S. 128, 140 (1990) ("If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more."); Terry v. Ohio, 392 U.S. 1, 19 (1968) ("The scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible." (internal quotation marks omitted)).

339 395 U.S. 752 (1969), *abrogated as noted by* Davis v. United States, 131 S. Ct. 2419 (2011).

340 *Id.* at 763 (internal quotation marks omitted). Note that the Court did not define a new exception here. Rather, it reexamined the doctrine because it lacked a solid normative basis. The decision to narrow the scope of the doctrine to bring it into line with the normative rationale for the exception is basically the same decision, as far as the scope is concerned, with recognizing a new exception narrowly because they are reaffirming the normative value of the exception.

341 *Id.* at 762–63.

342 Maryland v. Buie, 494 U.S. 325 (1990).

principle would have been modified to include a search where there is potential danger.

In *New York v. Belton*,[343] the Court applied *Chimel* to automobiles:

> While the *Chimel* case established that a search incident to an arrest may not stray beyond the area within the immediate control of the arrestee, courts have found no workable definition of "the area within the immediate control of the arrestee" when that area arguably includes the interior of an automobile and the arrestee is its recent occupant.[344]

The end result was a justification for searching the entire car,[345] but the reasoning is key. Previously, the Court had reasoned that there was a "reduced expectation of privacy" in automobiles, partially because they travel on public roads.[346] In *Belton*, though, the rationale from *Chimel*—with its associated scope limitations—was imported in full, rather then starting from the reduced privacy assumption.[347] Both the car and the home were contexts in which there was some right to privacy, and the Court recognized that because the rationale for intruding on them was the same, so should the scope limitations be.[348] Of course, police regularly abused this decision, arresting people for traffic violations and searching the car after they no longer posed a danger; but in *Arizona v. Gant*,[349] the Court performed a recalibration similar to *Chimel* itself.[350] Once an arrestee is secured and outside the vehicle, the danger justification disappears, and after *Gant*, the police may not search the vehicle unless there is probable cause that there is evidence related to the crime for which the person is being arrested.[351]

The particularity and timing requirements for warrants are another area where the scope is limited.[352] For a search warrant to be valid, it must specify a place and time for the search.[353] The scope cannot exceed what is listed, though once the search is properly underway, the plain view doctrine and further warrant exceptions do apply to information

---

343 453 U.S. 454 (1981), *abrogated as noted by Davis*, 131 S. Ct. 2419.

344 *Id.* at 460.

345 *Id.* at 460–61.

346 California v. Carney, 471 U.S. 386, 392 (1985).

347 *Belton*, 453 U.S. at 457.

348 In *Chimel*, the Court did address whether it mattered that the arrestee was secured, but presumably that changes the area "within his immediate control." Chimel v. California, 395 U.S. 763 (1969) (internal quotation marks omitted), *abrogated as noted by Davis*, 131 S. Ct. 2419.

349 556 U.S. 332 (2009).

350 *Id.*

351 *Id.*

352 KAMISAR ET AL., *supra* note 121, at 306–09.

353 Although it is not constitutionally required, many states limit the execution of warrants to daytime and to a short time window—usually ten days—after they are issued. *Id.* at 308–09.

gathered beyond its scope.[354] Like the danger and destructible evidence rationales, a warrant invites an intrusion to a place in which police are not otherwise expected, and the intrusion is appropriately limited according to those facts justifying it.

The similarity between these scope limitations is their focus on space and time. How do these limitations relate to social contexts, rather than spatial? *Katz* said that the Fourth Amendment governs "people, not places,"[355] and yet a strong focus on the home persists today.[356] The connection is that a location-based theory of the Fourth Amendment and a contextual theory overlap. Society has "overriding respect for the sanctity of the home," a person's only place where she can escape the outside world.[357] Therefore, it is not just a place, but also a social context, and it deserves its own protection.[358] As Justice Kagan observed in her *Jardines* concurrence, had the majority's trespass-based opinion turned instead on privacy interests, the opinion would have looked much the same.[359]

The same can also be said of the automobile.[360] Americans spend hours upon hours in the car, and to the extent that people expect to encounter police, it is for speeding tickets and other traffic violations, rather than a full-blown search.[361] Encounters should be limited to those citations, unless there is a good reason for further intrusion. Scope limitations are contextual limitations in that they limit searches in the social and spatial contexts where people do not expect interaction with police otherwise.

The opposite is true of searches in prison. Prison, too, is both a location and a unique social context, though one in which the Court decided there was *no* privacy interest:

---

354 Horton v. California, 496 U.S. 128, 134 (1990).

355 Katz v. United States, 389 U.S. 347, 351 (1967).

356 Kyllo v. United States, 533 U.S. 27, 38 (2001).

357 Payton v. New York, 445 U.S. 573, 601 (1980).

358 *See* Strandburg, *supra* note 32, at 659 ("While undertheorized, the special solicitude for the home . . . appears to have its roots in a number of social functions these places perform that enhance substantive privacy and intimate association.").

359 Florida v. Jardines, 133 S. Ct. 1409, 1418 (2013) (Kagan, J., concurring). She continued: "It is not surprising that in a case involving a search of a home, property concepts and privacy concepts should so align. The law of property 'naturally enough influence[s]' our 'shared social expectations' of what places should be free from governmental incursions." *Id.* at 1419 (alteration in original) (quoting Georgia v Randolph, 547 U.S. 103, 111 (2006)).

360 Arizona v. Gant, 556 U.S. 332, 343 (2009) (referring to "circumstances unique to the vehicle context").

361 Well, that is, unless a driver is accustomed to being pulled over based on racial bias, but searches on that basis are not exactly what we should be basing search doctrine on. *See* DAVID A. HARRIS, AM. CIVIL LIBERTIES UNION, DRIVING WHILE BLACK: RACIAL PROFILING ON OUR NATION'S HIGHWAYS (1999), *available at* http://www.aclu.org/racial-justice/driving-while-black-racial-profiling-our-nations-highways.

> A right of privacy in traditional Fourth Amendment terms is fundamentally incompatible with the close and continual surveillance of inmates and their cells required to ensure institutional security and internal order. We are satisfied that society would insist that the prisoner's expectation of privacy always yield to what must be considered the paramount interest in institutional security. We believe that it is accepted by our society that "[l]oss of freedom of choice and privacy are inherent incidents of confinement."[362]

Spatial contexts that overlap with social contexts are the exception, existing on both extremes of the privacy spectrum. The next doctrines are less spatially tied.

B. *Stops*

A "stop" is a noncustodial seizure of a person under the Fourth Amendment.[363] A legal stop requires reasonable suspicion of a crime.[364] Whether a particular encounter counts as a stop is a question that incorporates an awareness of social context.[365] As a threshold matter, if the police use physical force, the encounter is a stop in every case.[366] If a person consents to talking with the police voluntarily, it is not a stop. The interesting question is when a show of authority by police overrides consent. *California v. Hodari D.*[367] established the rule that as long as a reasonable person would feel he was free to "disregard the police and go about his business," the show of authority was not great enough to constitute a stop.[368] This is a rule heavily steeped in social context. Shows of authority include brandishing a weapon,[369] visibly displaying badges,[370] and yelling "Stop, in the name of the law!"[371]—basically those things that would inform a reasonable person that he should submit.[372]

Both the appearance of authority and likelihood of submission vary depending on context. Walking down the street, minding one's own business, would require a greater showing to convince a person to stop than if the person were a student in a school or on the road driving a

---

362 Hudson v. Palmer, 468 U.S. 517, 527–28 (1984) (alteration in original) (footnote omitted) (quoting Bell v. Wolfish, 441 U.S. 520, 537 (1979)).

363 *See* Terry v. Ohio, 392 U.S. 1, 16–17 (1968).

364 *Id.* at 21–22.

365 The doctrine is governed primarily by *California v. Hodari D.*, 499 U.S. 621 (1991) and *Florida v. Bostick*, 501 U.S. 429 (1991).

366 *Hodari D.*, 499 U.S. at 625.

367 499 U.S. 621 (1991).

368 *Id.* at 628.

369 United States v. Drayton, 536 U.S. 194, 205 (2002).

370 *Bostick*, 501 U.S. at 446 (Marshall, J., dissenting).

371 *Hodari D.*, 499 U.S. at 626.

372 *Id.*

car. In *Florida v. Bostick*,[373] the Court held that "to determine whether a particular encounter constitutes a seizure, a court must consider all the circumstances surrounding the encounter to determine whether the police conduct would have communicated to a reasonable person that the person was not free to decline the officers' requests or otherwise terminate the encounter."[374] The rule treats context as determinative, whether walking on foot or traveling on a bus with no exit.

C. *Administrative Warrants and Special Needs Searches*

The Fourth Amendment permits a class of administrative searches based on less than the individualized probable cause needed to obtain a criminal search warrant.[375] Administrative searches are premised on special needs that cannot be met by traditional criminal investigation, justified "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[376] Examples include inspections of housing for compliance fire and health code,[377] border searches,[378] searches of students in schools,[379] and airport security screenings.[380] Each of these search types is, at least formally, restricted tightly to its justification, and thus its context. While the Court has arguably been more liberal with granting new exceptions than is warranted,[381] the formal justification's reliance on context illustrates its importance to this doctrine.

The framework for administrative searches comes from *Camara v. Municipal Court of the City and County of San Francisco*,[382] in which the Court held that safety inspections of housing required an administrative warrant, based on "reasonable legislative or administrative standards for conducting an area inspection" rather than individualized probable cause.[383] The Court's definition of reasonableness "balanc[es] the need to search against the invasion which the search entails."[384] The Court put forth three factors comprising the test: 1) the long judicial and

373 501 U.S. 429 (1991).
374 *Id.*
375 *See* Camara v. Mun. Court of S.F., 387 U.S. 538 (1967).
376 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).
377 *Camara*, 387 U.S. at 538.
378 United States v. Martinez-Fuerte, 428 U.S. 543, 545 (1976).
379 *T.L.O.*, 469 U.S. at 341.
380 *E.g.*, United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007).
381 *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 255–56, 257 nn.14–15 (collecting critiques of the practical results of administrative search cases).
382 387 U.S. 523 (1967).
383 *Id.* at 538.
384 *Id.* at 537.

public acceptance of a practice, 2) public necessity coupled with an inability to accomplish the goal any other way, and 3) a limited invasion of privacy because the "inspections are neither personal in nature nor aimed at the discovery of evidence of crime."[385] This balancing test could have come from contextual integrity directly. The first factor suggests that the search complies with informational norms, the second factor goes to the normative layer, and the third explicitly states that the search cannot bleed over into an attribute—general criminal investigation—for which it is not intended.

The explicit recognition of social context pervades these cases. Holding that students can be searched in schools under a reasonable basis standard, the Court distinguished the criminal context from the school context, noting that the adversarial relationships between police and suspects do not exist between teachers and students, and that a mutual interest in furthering the goals of the educational context means that the teachers may assure "discipline and order."[386] In the context of government employment, the Court recognized that while "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer[,]"[387] searches "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."[388] Vehicle checkpoints are authorized with the recognition that the context of driving is different than the home, both because cars are highly regulated and generally because they are less sacrosanct than the home.[389] Fixed checkpoints can be used for sobriety checks[390] and immigration checks near borders,[391] but those are not good enough reasons to get an administrative warrant to search a person's home.

Even different types of administrative searches differ based on social context. The requirement of a warrant for housing inspections is relaxed in the context of highly regulated businesses, though not for just any business.[392] Businesses with liquor licenses do not receive as much Fourth Amendment protection,[393] nor do auto junkyards[394] or sellers of

---

385 *Id.*

386 New Jersey v. T.L.O., 469 U.S. 325, 331, 350 (1995).

387 O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

388 *Id.* at 725.

389 California v. Carney, 471 U.S. 386, 392 (1985).

390 Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990).

391 United States v. Martinez-Fuerte, 428 U.S. 543, 545 (1976).

392 Marshall v. Barlow's Inc., 436 U.S. 307, 309–12 (1978). This suggests that perhaps the "chemical market" context is just as salient as the "market" context in *United States v. Knotts*, 460 U.S. 276 (1982), though "highly regulated businesses" might be the correct context. See discussion of *Knotts*, *supra* Part III.C.

393 Colonnade Catering Corp. v. United States, 397 U.S. 72 (1970).

394 New York v. Burger, 482 U.S. 691 (1987).

firearms during business hours.[395] Vehicle checkpoints for immigration checks are restricted to those places where motorists might expect it[396]—that is, at the border[397]—while sobriety checkpoints are not so restricted.[398] This is purportedly because the fear engendered by random stops for immigration papers is intrusive and threatening in a way that interaction with the police for a sobriety check is not.[399] That is, the attribute at issue results in different worries about the encounter and thus different transmission principles.

D. *Police Exposures to Third Parties*

Because administrative warrants are issued for specific purposes, the police cannot also use them for criminal investigations.[400] It turns out that the reverse is also true: police may not take a search warrant that is meant for criminal investigation and allow unrelated people to obtain the fruits of it. Police may not expose the inside of the home to third parties not "related to the objectives of the authorized intrusion."[401] In *Wilson v. Layne*,[402] the Court ruled unanimously in that a media ride-along by *Washington Post* reporters violated the Fourth Amendment.[403] The ruling was not simply that third parties were forbidden from attending the police during a search. It was subtler than that and context-based:

> Respondents concede that the reporters did not engage in the execution of the warrant, and did not assist the police in their task. The reporters therefore were not present for any reason related to the justification for police entry . . . . Where the police enter a home under the authority of a warrant to search for stolen property, the presence of third parties for the purpose of identifying the stolen property has long been approved by this Court and our common-law tradition.[404]

---

395 United States v. Biswell, 406 U.S. 311 (1972).

396 *Martinez-Fuerte*, 428 U.S. at 559; Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973) (holding in part that a search based on a roving patrol could not have been a "border search"); *see also id.* at 275 (Powell, J., concurring).

397 United States v. Ortiz, 422 U.S. 891, 896–97 (1975) ("[A]t traffic checkpoints removed from the border and its functional equivalents, officers may not search private vehicles without consent or probable cause.").

398 Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990).

399 *See Ortiz*, 422 U.S. at 897; *id.* at 895 (Rehnquist, J., concurring).

400 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

401 Wilson v. Layne, 526 U.S. 603, 611 (1999).

402 526 U.S. 603 (1999).

403 *Id.* at 605.

404 *Id.* at 611–12.

A total ban on third parties attending a search would make law enforcement's job more difficult, and once there is a warrant, the law enforcement context is most salient. Thus, in the normative evaluation, rules narrowly tailored to aid the investigation will be preferred because they are in line with the values of the relevant context. The police are there for investigation, so they are allowed to bring people in and do things related to their work and that work only.[405] The Court had been explicit about this principle earlier,[406] but this case provides the most concrete example.

CONCLUSION

This Article has proposed that we reinterpret Fourth Amendment search doctrine to assign context its proper place in the theory. If one believes both that contextual integrity does a good job of describing how people in liberal societies experience privacy, and that the Fourth Amendment means to enact a prohibition on the police unreasonably invading a "reasonable expectation of privacy," then this approach should be appealing. The centrality of context would also unify Fourth Amendment theory; as Part V illustrates, it is already central to other parts of the doctrine.

Contextual search is not without its practical difficulties. If enacted today, it would radically alter established Fourth Amendment law, potentially unsettling search law for a long time. Relatedly, if the reforms in this Article were implemented all at once, many police actions would suddenly become searches subject to the Fourth Amendment. While many such searches would be considered reasonable and equally as permissible as they are today, they would first have to be litigated, temporarily creating a greater burden on an already strained criminal justice system.

The Article has also left open many normative questions—deciding when searches are or are not reasonable. As discussed, contextual search is not equipped to make that determination; it can only provide guidelines to frame the debate and teach us that consideration of the context is paramount.[407] Because of this limitation, contextual search

---

405 *Id.*

406 Maryland v. Garrison, 480 U.S. 79, 87 (1987) ("[T]he purposes justifying a police search strictly limit the permissible extent of the search . . . .").

407 This Article is in fact agnostic as to the outcome of those normative debates. If Facebook founder Mark Zuckerburg has his way and social norms become much more open, a context-based Fourth Amendment would reflect that. Emma Barnett, *Facebook's Mark Zuckerberg Says Privacy Is No Longer a 'Social Norm*,' THE TELEGRAPH (Jan. 11, 2010, 12:55 PM), http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html.

implicitly relies on the "wisdom of the common law" to sort out these questions.

Given the potential for unsettled doctrine, the important question is whether the current state of settled doctrine is better or worse than an unsettled doctrine that is much more responsive to the realities of privacy perception. The Article already discussed the internal inconsistencies of current doctrine, but its practical effects are dangerous. If third-party doctrine continues as is, email, text messages, any documents stored online—basically any digital communication—will be outside the purview of the Fourth Amendment, despite more and more lives actually being lived online.[408] Today, as each new technology is developed, there are no constraints on police who want to use it, except if it invades constitutionally protected areas like the home.[409] Coupled with the recent decision by the Supreme Court that the good faith exception applies to the exclusionary rule,[410] there is just no incentive for police to refrain from using every privacy-invading advantage they can get until it is declared off-limits by a court. The doctrine is in need of a little unsettling.

While the discussion only mentioned it tangentially, contextual search doctrine implicitly relies on a proportionality principle for reasonableness of search, which might well be an administrative nightmare. In practice, because clarity in search is important (or at least as much clarity as it is even possible to achieve),[411] a proportionality principle would take the form of several discrete levels of suspicion required for the police to take a certain action. Fundamentally, such a discrete proportionality principle is already in place, but not recognized as such and is more limited than it should be. As Christopher Slobogin has observed:

> The Court abandoned the single probable cause standard because it was too difficult to meet in situations where the state had a legitimate interest in acting because of the lesser intrusion involved. And [the Court abandoned] the two-tiered approach, because it has been confronted with searches and seizures it views to be even less intrusive, as the drug testing and roadblock cases show. At the same time, because it is still officially wedded to the probable cause and reasonable suspicion standards for most cases, the Court is prevented, at least technically, from requiring *more* certainty than probable cause for particularly intrusive investigative techniques. From a deontological perspective, the proportionality principle is

408 Strandburg, *supra* note 32, at 616–17.

409 *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

410 Davis v. United States, 131 S. Ct. 2419 (2011).

411 Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 68–75 (proposing such a sliding scale approach).

> essential to establishing a sound regulatory framework for searches and seizures.[412]

A proportionality principle, then, would just take probable cause as one point in the proportionality spectrum, specifically the point at which a warrant will issue.[413]

With the explicit recognition of multiple levels of suspicion, *more* clarity could be achieved, instead of the Court defining probable cause alternatively as a "fair probability,"[414] "substantial chance,"[415] or "reasonable ground for belief of guilt,"[416] the end result of which is that each standard can be applied to any set of facts, with no clarity at all.[417]

The concurring Justices in *Jones* followed their intuitions that long-term surveillance implicated the Fourth Amendment, even though it only captured what was seemingly available to the public eye.[418] The executive branch, meanwhile, has begun to accept that context is central to privacy. Both President Barack Obama's Privacy Bill of Rights[419] and the Federal Trade Commission's 2012 report on consumer privacy[420] heavily rely on Professor Nissenbaum's theory in making their privacy recommendations.[421] The judicial branch can now take their next cue from the executive. While other privacy theories can explain the difference between GPS and a beeper, contextual integrity provides the best toolbox to ensure that the Fourth Amendment remains grounded

---

412 *Id.* at 70–71 (footnotes omitted).

413 A proportionality principle also fits nicely with the original meaning of the Fourth Amendment as described by Akhil Reed Amar. Professor Amar noted that, originally, the question of a search's permissibility only focused on reasonableness, and that warrants were grants of immunity to the police from civil liability. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 778 (1994). A proportionality principle also focuses on reasonableness separately from warrants, so the function of warrants could either be as a further restriction—probable cause plus, as it were—or they could return to serving this function, assuming the qualified immunity doctrine's scope is reduced.

414 Illinois v. Gates, 462 U.S. 213, 238 (1983).

415 *Id.* at 243 n.13. It is pretty remarkable that two different definitions of probable cause actually exist in the same case.

416 Maryland v. Pringle, 540 U.S 366, 371 (2003) (internal quotation marks omitted).

417 *See* Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789 (2013).

418 United States v. Jones, 132 S. Ct. 945, 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

419 THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY 15–18 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

420 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

421 Alexis Madrigal, *The Philosopher Whose Fingerprints Are All over the FTC's New Approach to Privacy*, THE ATLANTIC (Mar. 29, 2012, 4:44 PM), http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365.

in society's actual experience of privacy, and that is what "reasonable" means.