Contextual Expectations of Privacy

Andrew Selbst, New York University

Available at: https://works.bepress.com/andrew_selbst/1/
CONTEXTUAL EXPECTATIONS OF PRIVACY

Andrew D. Selbst*

Fourth Amendment search jurisprudence is nominally based on a “reasonable expectation of privacy,” but actual doctrine is detached 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.” Over the last decade, privacy theorists have begun to understand that a consideration of 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 important differences between banking and

* Privacy Research Fellow, New York University Information Law Institute, Postdoctoral Research Fellow, Department of Media, Culture and Communications; J.D. 2011, University of Michigan Law School; M.Eng. 2005, S.B. 2004, Massachusetts Institute of Technology. Special thanks to the faculty and 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 throughout the past year. 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 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.
other settings. In United States v. Jones, the recent GPS case, the five concurring justices demonstrated a willingness to consider new approaches to search, but they lacked the language and framework with 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.

Introduction

I. Contextual Integrity
   A. An Introduction to Contextual Integrity
   B. Contextual Integrity and the Fourth Amendment
II. The Katz Paradigm and its Problems
   A. The Instability of Katz
   B. State Action and the Divergent Meanings of "Search"
   C. Lack of Clarity in the Normative Test
III. Search Doctrine As Contextual Integrity
   A. Information Relayed to Third Parties
   B. Informants and “Pretend Friends”
   C. Privacy in Public
   D. Emanations
   E. Roving Wiretaps
IV. Putting Context in Context
   A. Scope Limitations and Spatiotemporal Context
   B. Stops
   C. Administrative Warrants and Special Needs Searches
   D. Third-Party Exposures by Police
V. Technology and the Future of Search Litigation
   A. Cell Phone Location Data
   B. Pervasive Visual Surveillance and Recording
   C. Online Social Networks
Conclusion

INTRODUCTION

On January 23, 2012, with a mighty stroke of its word processors, the Supreme Court changed Fourth Amendment jurisprudence forever . . .
maybe. The truth is that in the wake of United States v. Jones,¹ no one really knows what will happen to the Fourth Amendment’s search doctrine. 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, contradicting 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.² 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,”³ but they did not articulate much of a theory as to why.⁴ Instead Justice Alito called for legislative answers to privacy protections, essentially pleading judicial incompetence.⁵ Meanwhile, Justice Alito’s suggestion that society’s privacy expectations are vanishing is perhaps the most frightening for privacy advocates.⁶ While privacy attitudes certainly change over time, this blithe statement reflects a failure of imagination. The Court is still saddled with reductionist understandings of privacy that boil down to the familiar dichotomy: Is a piece of information private or public?⁷

While Justice Alito’s reference to diminishing privacy is disturbing, the concurring justices get at least one thing exactly right: most of the surveillance technology being deployed or used now – cell site monitoring, drones, automatic license plate recognition, surveillance cameras, and social networks do not need physical access to work.⁸ Thus, while the majority’s reliance on trespass is surely meaningful for other reasons, such as perhaps searches of trash bins,⁹ the Katz test – and thus the Court’s understanding of

---

² Id. at 949 (“It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a “search” within the meaning of the Fourth Amendment when it was adopted.”)
³ Id. at 955, (Sotomayor, J., concurring), 964 (Alito, J., concurring).
⁴ 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), 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.”)
⁵ Jones, 132 S.Ct. at 964 (Alito, J., concurring) (“In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”) (citation omitted)
⁶ Id.
⁷ Jones, 132 S.Ct at 963.
⁸ Julia Angwin, FBI Turns Off Thousands of GPS Devices After Supreme Court
privacy – is still central to search doctrine. Indeed, the Court twice stressed that the trespass test supplements rather than supplants the *Katz* test, and Justice Sotomayor seemed to rely on that assurance to even sign on.

The justices may be forgiven for misunderstanding the nature of privacy. Defining a right to privacy has proven a monumentally difficult task. Various formulations have been proposed, including Warren and Brandeis’s famous “right to be let alone,” the right to secrecy, control over personal information, a right to intimacy, and a right to personal autonomy. Legal definitions in particular tend to focus on binary distinctions, presumably because they provide relatively easy lines to draw in court. Specific definitions of “private” and “public” differ depending on who is asked, with no agreement between different areas of consideration.

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 of intimate. The one similarity between all the theories is the reason they all fall short: they are all dichotomies.

Each of these dichotomies has proven inadequate. None of the binary distinctions can quite capture what society means by the concept of “privacy.” In tort law, for example, four different “privacy torts” are required because no single one will do. In public view, where before *Jones* everyone thought we have no “reasonable expectation of privacy” in our whereabouts, stalking someone is still a pretty clear privacy violation. In social relationships, people often share information with others that they

---


9 *Jones*, 132 S.Ct. at 952 (“[A]s we have discussed, the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”), 953 (“[U]nlike the concurrence, which would make Katz the exclusive test, we do not make trespass the exclusive test.”).

10 *Id.* at 954 (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.'” (citations omitted))


14 Solove, supra note 11, at 1109.


17 HELEN NISSENBAUM, PRIVACY IN CONTEXT 89-98 (2009).

18 *Id.* at 90.

wish kept private from the world at large. In fact, the degree of sharing is one of the primary factors defining social relationships. Most importantly for the future, technology consistently throws wrinkles into even those binaries people thought they understood. Are shopping habits private or public? On the internet consumers are constantly tracked, often leading to useful recommendations at Netflix and amazon.com, but most people would call security if they were followed around a department store for two hours. Court records are presumptively public, but there is a big difference between having to go to the courthouse and dig through files and a simple no-cost web search open to potential employers, insurance companies, and romantic interests. 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 all-or-nothing terms often erroneously claim that young people today just do not care about privacy, when in reality, they merely conceive of it differently.

The problem with binaries is that to employ them is to attempt the impossible—simplifying privacy by abstracting away the context. Recent privacy law scholarship, particularly over the last decade, has focused a great deal on privacy theories derived from social context. Early on, 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. 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.” Orin Kerr argued that the Supreme Court was unwittingly using context-dependent theories of the Fourth Amendment, and then argued that doing so makes perfect sense because nothing else will work. Lior Strahilevitz argued for

---

21 Amanda Conley, Anupam Datta, Helen Nissenbaum & and Divya Sharma, Sustaining both Privacy and Open Justice in the Transition from Local to Online Access to Court Records: A Multidisciplinary Inquiry 71 Md. L. Rev. ___ (forthcoming 2012).
22 Chris Jay Hoofnagle, et al., How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies? (2010)
24 Post, supra note 23, at 962.
25 Solove, supra note 11, at 1092.
26 Kerr, supra note 23, at 507.
27 Id. at 525.
a theory of privacy based on the practical likelihood of information dissemination given what we know about social networks. Katherine Strandburg has argued that privacy law should be sensitive to the “exploding variety of contexts” in social web applications. Now, even the executive branch of the federal government has embraced context, giving it the spotlight in the White House’s Privacy Bill of Rights and the Federal Trade Commission’s recent report on consumer privacy.

All this scholarship recognizes the importance of social context as well as the impossibility of a privacy definition excludes it. For Helen Nissenbaum’s theory of contextual integrity, however, privacy is not just related to context, but is instead defined as adherence to the informational norms that constitute the context. This Article uses Professor Nissenbaum’s theory to posit a context-based Fourth Amendment search doctrine. As she wrote in *Privacy in Context*, her book presenting the theory:

> The central thesis of this book is that a right to privacy is neither a right to secrecy nor a right to control, but a right to *appropriate* flow of 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.

With its focus on context, Professor Nissenbaum’s theory can give the “reasonable expectation of privacy” test a grounding it currently lacks. The main contribution of the theory is its descriptive power. Its application to the Fourth Amendment will bring the phrase “reasonable expectation of privacy” into line with how people in society actually experience privacy. Indeed, a focus on information flows in social contexts would make the

---

28. Strahilevitz, *supra* note 20, 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.”)


Fourth Amendment much more about “people, not places” than it is today. Additionally, while contextual integrity cannot, by itself, answer many of the resulting normative questions that arise in its application, it provides important constraints and structure to judicial decisionmaking that do not exist in current understanding.

Given the historical difficulties interpreting what society means by “privacy,” it makes sense that Fourth Amendment search doctrine, in which the threshold test is whether a person has a “reasonable expectation of privacy,” is itself in disarray. Various scholars have called the current state of the doctrine an “embarrassment,” “unstable,” and “a series of inconsistent and bizarre results that [the Supreme Court] has left entirely undefended.” If – as contextual integrity suggests – society’s concept of privacy is rooted in context, and the Fourth Amendment is based on society’s expectations of privacy, then it follows that the Fourth Amendment’s search doctrine should be rooted in context as well. To a certain extent, though the Court has never said so explicitly, it already is. As Professor Kerr noticed a few years ago, the Supreme Court’s approach to reasoning about search tends to vary based on the type of case and its relevant context. There are also many uses of context written into current law: scope limitations, third parties entering with police officers, and administrative searches, where the same action can be a Fourth Amendment violation or not, depending on whether the “government interest at stake exceed[s] those implicated in any ordinary law enforcement context.”

A context-focused doctrine provides a framework for the justices’ intuitions about long-term tracking and fixes many of the inconsistencies in current jurisprudence. The 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-

37 Kerr, supra note 23, at 507. Kerr suggests that there are four different approaches that the Supreme Court takes, and thus limits his analysis to four a posteriori contextual categories. While I agree with the observation that the Court uses context more than it has ever explicitly recognized, I disagree with his resulting approach, preferring a theory in which context is central to the reasoning, rather than an observed phenomenon.
38 See Wilson v. Layne, 526 U.S. 303 (1999) (forbidding reporters to enter on the same warrant as police).
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. This normative approach maps roughly to the exceptions to the warrant requirement, such as exigency or officer safety, which exist when there is a good justification to disrupt society’s expectations. While contextual integrity does not itself possess the tools to make determinations about the correct normative outcome, the normative component gives guidelines as to what information is relevant to consider, helping to constrain the decision-making process.

Part II gives an overview of the current search doctrine under the Katz “reasonable expectation of privacy” test and examines how some of its difficulties will be addressed by viewing the test as an application of contextual integrity. Part III examines 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 integrity, with an eye toward illustrating the general structure of such analysis. Part IV finds areas in current Fourth Amendment jurisprudence where context is implicitly recognized, though not labeled as such. The discussion demonstrates that a context-conscious doctrine would pull together previously disjoint pieces of current doctrine under a more unified theory.

Part V 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, and suggests a doctrinal approach to them under the theory developed here.

I. CONTEXTUAL INTEGRITY

Contextual integrity is a theory describing how contemporary liberal societies view privacy on the ground. It is an attempt to answer what has always been a very difficult question by observing the impossibility of reductionist thinking about privacy, too often employed to discuss privacy in terms of binaries such as public and private. It contends that the reason it has been difficult to reach consensus about how to draw the line between public and private, or even about what those concepts mean, is that they overlap and differ by social context. While contextual integrity is not a legal theory, its common law-like structure lends itself very well to incorporation into American jurisprudence. This section first describes the theory and
discusses how it interfaces with the Fourth Amendment.

A. An Introduction to Contextual Integrity

The theory of contextual integrity contends that society’s implicit understanding of privacy is respect for the appropriate flow of information about identifiable persons within particular social contexts. The principle of appropriateness is quite 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 between and among social actors within a given social context. 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 is so called because it relies on the background assumption that social contexts are an organizing principle of social life. 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.” These “[c]ontexts are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).” In modern industrial societies, familiar contexts include healthcare, the marketplace, finance, politics, religion, education, friends, and home life. Each of these contexts has its own set of informational norms that govern the relationship between actors and information.

There are three component parts to an informational norm: actors, attributes, and transmission principles. Actors can be subjects, senders, or receivers of the information. Attributes are what the information is about – whether it is a health record, name of an associate, location, or piece of gossip, for example. Transmission principles are restrictions placed upon the flow of information between the actors by the particular context – the

---

40 Nissenbaum, supra note 17, at 127. Information flow is comprised of sharing, capture, disclosure, communication, and dissemination of information.

41 Id. at 129.

42 This is a widely accepted position of established social theory, though with different particular views. Contextual integrity is agnostic as to these particulars. Id. at 130-32.

43 Id. at 129-30.

44 Id. at 132.

45 Id. at 130.
“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, shared in confidence, obtained with authorization, obtained under compulsion, held in fiduciary care, sent for a specific limited purpose, or obtained with a warrant.46 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 derive) – matter simultaneously, allowing for a wider range of possibilities than other accounts acknowledge. 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 IRS in an annual tax return will be sent only to the appropriate parties as described in law. Additionally, because informational norms derive from their social context, their structures vary. Informational norms, much like law itself, can vary between fully specified rules and basic principles. The sources of norms can be law, professional codes, or merely ideas implicitly woven into “the fabric of social and political life.”47

The structure is best illustrated with an example. In the healthcare context, a patient will often share information with a doctor for the purpose of healthcare. The doctor will then share information with other members of her staff – hospital administrators, other doctors, or nurses. When the doctor shares with a nurse, the doctor is the sender, sharing information with the nurse as receiver, about the patient as 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. However, if the doctor shared medical information with the patient’s employer, that would violate the informational norm. Note 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.

The value of norms is that they characterize the expected, or “normal” flow of information, but if contextual integrity could only provide a static descriptive assessment of whether a norm had been violated, it

46 Id. at 145.
47 Id. at 128.
would be incomplete. To carry moral weight, the theory must include a way to distinguish between advances in law or technology that could be seen as beneficial in the balance and those that are harmful. Thus, contextual integrity includes a normative layer in addition to the descriptive layer described thus far, allowing the theory to both call attention to disruptions in established information flows and to provide a lens through which to evaluate these disruptions in moral and political terms.

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 and unfair discrimination are all effects to consider.\textsuperscript{48} 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 context, and then considers the value of the context itself to society. 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 is rapidly disrupting information flows. Full consideration must be given, then, 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 of which are foundational values of the healthcare context. If changes in the information flow lead patients to avoid tests or lie to physicians, then these ends and values are undercut, and the new flows cannot be supported, even if generalized moral and political considerations are a wash. Similarly, a rule that information relayed to banks will be shared with police automatically changes the entrenched values in banking enough that it is important to consider whether society wants to condition use of the financial system on waiver of privacy rights.\textsuperscript{49} The answer might be yes, but the important point, often overlooked by other theories of privacy, is that the effect on the financial context itself should be central to the normative consideration.

One important and quite difficult question in applying contextual

\textsuperscript{48} 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 17, at 74-88.

\textsuperscript{49} 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); see also text accompanying infra note 118.
Integrity is how to choose the appropriate 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 required to do by law, 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. Thus, arguments about the values often appear as arguments about the relevant context. Rather than being a fatal flaw of the theory, this unavoidable reality merely makes the decision about context iterative. If an analyst considers the most plausible contexts, different rules emerge, and the normative debate will proceed with more variables. The eventual choice of best rule is defended in part by the correct choice of context. In many cases, the context is fairly well understood, but as with anything else, borderline cases are going to be hard, and contextual integrity’s application in the law will ultimately have to be resolved by judge or jury.

Implicitly, 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. Only if a new practice is normatively preferred after being compared with the old, will that practice will be incorporated into the framework of that context for the future as an amendment to the transmission principle going forward. As a result of this similarity, contextual integrity functions well as a theoretical foundation for a common law doctrine. This stare decisis element also makes the iteration in choosing a context less troubling, because the theory inherently modifies itself it a similarly iterative fashion.

Michael Birnhack describes this as a flaw of contextual integrity, though I do not believe it is fatal. Michael D. Birnhack, A Quest for a Theory of Privacy: Context and Control, 51 JURIMETRICS J. 447, ___ (2011) (reviewing NISSENBaUM, supra note 17) (“[D]efining a context becomes a process subject to the interpretation of the observer (or perhaps manipulation by an interested party).”). Rather, I just think it makes the process iterative. If the analyst chooses one or two plausible contexts, different rules emerge, and a judge or jury can choose between those rules. The eventually choice of best rule than reconfirms the context.

If the relevant inquiry is a “reasonable expectation” – an inherently social question – than 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.

See Planned Parenthood of Southeastern Penn. v. Casey, 505 U.S. 833, 854-55 (1992) (discussing that stare decisis is a strong presumption, but not quite an “inexorable command”).
B. Contextual Integrity and the Fourth Amendment

The Fourth Amendment to the Constitution reads: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . .”54 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 it reasonable?55 If a court finds that the action was not a search at all—that is, that there was no “reasonable expectation of privacy,”56 (and that there was no government trespass)57—then the Fourth Amendment simply does not apply, and the query has ended.58 If, however, the action was legally a search, then the doctrine requires that the search be justified either with a valid warrant or a judgment that the action falls into one or more of the recognized exceptions to the warrant requirement, coupled with the appropriate level of suspicion for the search (e.g. probable cause (PC) or reasonable, articulable, particularized suspicion (RAPS)). If the police had no warrant and the action either did not belong in one of the recognized warrant exceptions or was not accompanied by the requisite level of suspicion, then a Fourth Amendment violation has occurred.

Contextual integrity’s two layers represent a shift from this approach. The descriptive layer first asks the question of whether informational norms were violated, which is similar, but not quite identical to the doctrinal question of whether there was a “search.” The descriptive layer can be broken down further into two parts: the “framework analysis” and the “violation inquiry.” The framework analysis essentially answers the question: Is there a “reasonable expectation of privacy?,” or more specifically, “Under what circumstances is there a reasonable expectation of privacy in this social context?” The framework is defined by its constituent parts: the actors, information types, and transmission principles. 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 – that is, the “reasonable expectation of privacy” – were actually violated. If the

54 U.S. CONST. amend. IV.
57 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. 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.")
58 See sources cited supra note 55.
norms were violated, then that is a prima facie violation of contextual integrity.\textsuperscript{59} Therefore the result of the descriptive layer is whether something was a “search” under the \textit{Katz} test.

Unlike current doctrine, however, at no point in contextual integrity’s descriptive analysis does the theory ask whether there was a “search,” though it does address whether there was a “reasonable expectation of privacy.” Therefore, in the framework proposed by this Article, “search” will have to mean something different than it currently does. Specifically, when a police officer “searches,” the officer is literally seeking information, taking an action to change information flows. Law already contains this concept: state action. State action serves to separate the informant who goes to the police because he is feeling guilty from the one coaxed by the police into informing. State action separates the police officer unintentionally witnessing a crime from the one investigating.\textsuperscript{60} In current doctrine, state action is suppressed because it is implicit and no case would ever get to the Supreme Court without it. Meanwhile, the search requirement is broader, encompassing both state action and those situations in which there is no reasonable expectation of privacy. In natural language, however, a “search” is nothing more than the action of searching, which is presumably why text of the Fourth Amendment does not define it as a standalone concept.\textsuperscript{61} Because a) in this article’s formulation, contextual integrity completely occupies the concept of reasonable expectation of privacy, b) state action is still a necessary limitation on the Fourth Amendment, and c) the natural language definition of search is state action, the definition of “search” here is rolled back to mirror state action doctrine.\textsuperscript{62} Separately, a “reasonable expectation of privacy” is still the touchstone test for whether a Fourth Amendment violation has occurred. Thus, a Fourth Amendment violation is a search (state action) that causes a contextual integrity violation (violation of the reasonable expectation of

\textsuperscript{59} The two parts are analogous to the “law” and the “facts” of the descriptive layer.

\textsuperscript{60} California v. Greenwood, 486 U.S. 35, 41 (1988) (“\textit{[P]}olice cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.”).

\textsuperscript{61} U.S. CONST. amend. IV.

\textsuperscript{62} State action doctrine is supposed to operate in the Fourth Amendment just like the First and Fourteenth. United States v. Jacobsen, 466 U.S. 109, 114 (1984) (“This Court has also consistently construed [Fourth Amendment] protection as proscribing only governmental action; it is wholly inapplicable “to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.”) However, because the modern doctrine defines search so narrowly, state action has largely been excised from search doctrine. While it is not the focus of this Article to reinstate state action in the Fourth Amendment, it turns out to be essential to the working of this theory.
privacy). Both state action and reasonable expectation of privacy are required in current doctrine and the proposed one.

Next comes the normative layer, which will ask both about the values affected by the different possible information flows and how the different flows affect the relevant contexts. The normative layer asks whether a given information flow disruption (read: search) was reasonable in a moral or political sense. Additionally, the normative analysis is required whether or not the violation inquiry finds a disruption; if there is a prima facie violation, contextual integrity asks about the disrupted information flow, but if there is no violation, it is also important to determine that the context is not too permissive. This symmetry is important for contextual integrity to argue 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.

Applying the normative analysis in Fourth Amendment cases is easier than in a more open-ended context 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 do their jobs, the liberty of citizens in their interaction with police, and community cohesiveness. These same values will appear again and again in these cases, because that is the nature of the normative Fourth Amendment inquiry.

An example should illustrate the differences in reasoning. In *Terry v. Ohio*\(^{63}\), a police officer stopped the defendants while they were walking down a public street, after he observed them for some time and became “thoroughly suspicious.”\(^{64}\) The police officer thought that the defendants were “casing a job” and worried that “they may have a gun.”\(^{65}\) The Supreme Court first determined that the frisking the defendants on the street was a search under the Fourth Amendment; that is, the defendants had a reasonable expectation of privacy about what was on their person while on a public street.\(^{66}\) Because it was a search, the second part of the inquiry was triggered: whether the search was “unreasonable.”\(^{67}\) The Court eventually concluded that when “an officer is justified in believing that the individual whose suspicious behavior he is investigating at close range is armed and presently dangerous to the officer or to others,” he may “neutralize the

\(^{63}\) 392 U.S. 1 (1967)
\(^{64}\) *Id.* at 6.
\(^{65}\) *Id.*
\(^{66}\) *Id.* at 9 (“Unquestionably petitioner was entitled to the protection of the Fourth Amendment as he walked down the street in Cleveland.”)
\(^{67}\) *Id.*
threat of physical harm.\textsuperscript{68} The Court further made clear that the scope of the search must be based on its context, confining the permissible search to “an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer.”\textsuperscript{69}

The contextual integrity approach would come to a similar conclusion. The context is someone walking down the street. The framework analysis identifies the relevant information flows constituted by the attributes, actors, and transmission principles. In \textit{Terry}, there is one relevant information flow. The \textit{subject} and \textit{sender} of the information is Terry, the defendant, and the \textit{receiver} is the police officer. The attribute is what the defendant is carrying on his person. The transmission principles here are well understood. If a random passerby either frisked Terry or even asked him for this information, society would view it as a breach of his privacy due to norms that permit people not to share that information. Police are often, but not always, in a situation where they are just like other citizens, except for their badge, and this would be one such scenario.\textsuperscript{70} Thus subject/sender is in control of the information flow to the police just like any other citizen, except if the police possess a valid warrant or recognized warrant exception coupled with an adequate level of suspicion.\textsuperscript{71} That is, if Terry chooses to inform the police officer, he is free to do so, and he alone possesses that option. Once the actors, attributes and transmission principles are determined, the framework analysis is ended, and the theory then proceeds to the violation inquiry, which examines the actual information flow. In this case, the officer searched in violation of the transmission

\textsuperscript{68} \textit{Id.} at 24.
\textsuperscript{69} \textit{Id.} at 29.
\textsuperscript{70} See Colb, \textit{supra} note 35, at 123. It is important to note that this is not always the case. The reasons for a norm are important. For instance, one of the reasons that society views following someone as a breach of privacy is the possibility that when someone is following another person, they mean them harm, or at least that the person being followed would be justifiably concerned about harm. If we object to police following us, it would be for a different reason, and thus the question really must be whether a transmission principle allows the \textit{police} to have a piece of information. That said, the “regular person + badge” model works most of the time as a shortcut.
\textsuperscript{71} Note here, and throughout this Article, that we are simply discussing the extremes of “no suspicion” and “warrant” or general “warrant exceptions.” We never discuss the appropriate level of suspicion. So \textit{Terry} ruled that reasonable suspicion of being in danger is required, but perhaps the correct ruling would have required PC instead. We do not take a position on that level of detail, except to say that it would likely either look like a sliding scale, where the depth of the intrusion necessitates a higher level of suspicion, or if that would prove completely unworkable, multiple discrete levels of suspicion. See Christopher Slobogin, \textit{The World Without a Fourth Amendment}, 39 UCLA L. REV. 1, 68-75 (proposing such a sliding scale approach); \textit{but see} Anthony G. Amsterdam, \textit{Perspectives on the Fourth Amendment}, 58 MINN. L. REV. 349, 393 (1974) (arguing that while a sliding scale would be the most ideal, it would be completely unworkable).
principles: Terry did not consent and the officer had no warrant. Thus, contextual integrity was violated, and the analysis proceeds to the normative layer.\textsuperscript{72} Note again that this is very similar to the classic Fourth Amendment approach, except that the warrant or established warrant exceptions were already considered; if a warrant existed or an exception applied, the transmission principle would not have been violated and no prima facie violation would have occurred.

The normative layer of the contextual integrity analysis asks whether the prima facie violation of the informational norms of the context – here a person walking down the street – is normatively desirable – that is, whether a new principle should apply. In \textit{Terry}, the question would be whether, and under what circumstances, it is normatively preferable, in light of the Fourth Amendment, to permit warrantless “stop-and-frisks.” A court performing the normative analysis would examine the interests and values at stake, which as mentioned earlier, include enabling police to do their jobs better, community trust of police, and liberty of citizens. \textit{Terry} is a relatively simple case because the values of the “walking down the street” context are as general as can be, reducing the query to standard Fourth Amendment normative questions. So here, a court would just balance the very same things as the Supreme Court did – the depth of the intrusion, versus the consequences of fewer police officers on balance because it would be a riskier job. Given the values considered were the same in both cases, the Court likely would have come out the same way after the normative layer.\textsuperscript{73}

\section{II. The \textit{Katz} Paradigm and Its Problems}

Though contextual integrity analysis has many of the same contours as current doctrine, the results are often different. A few phenomena drive these differences. First, the subjective and objective halves of “reasonable expectation of privacy” are often blended in current law, contributing to what scholars have called the “instability”\textsuperscript{74} or “circularity”\textsuperscript{75} of the \textit{Katz} doctrine. The confusion is an unfortunate result of the use of the word

\begin{itemize}
\item \textsuperscript{72} Today, because \textit{Terry} is already law, we would say instead that a \textit{Terry} stop is an additional part of the transmission principle, and thus that contextual integrity was not violated at all.
\item \textsuperscript{73} Whether the level of suspicion required for a \textit{Terry} stop should be RAPS (as it actually is now), or something else like PC is one potential point of disagreement, but one that lies beyond the scope of this Article.
\item \textsuperscript{74} Colb, \textit{supra} note 35, at 123.
\end{itemize}
“expectation” in both halves of the test, rather than something akin to a “privacy interest” in the objective test. Contextual integrity avoids this confusion naturally as a result of its analytical structure. Second and related is the Fourth Amendment’s distortion of the word “search,” which has separated doctrine from society’s actual expectations of privacy. Finally, courts often make normative judgments about whether one rule would be preferable to another. These judgments often pit officer certainty and bright line rules against a more nuanced approach and hazily defined rights. The normative structure of contextual integrity aids this process by more clearly identifying the particular values at stake in each decision, so that, however the decisions turn out, they are made for the right reasons and can be evaluated or reevaluated along those same lines. The contextual integrity approach will not answer the normative questions, but it will bring them to the foreground of the decisions so answers can be sought. The current variant of Fourth Amendment doctrine is not an inevitable byproduct of Katz or a privacy-focused regime. If contextual integrity is used to provide a framework, the doctrine can be made more consistent and in touch with society’s privacy norms.

A. The Circularity of Katz

The circularity of the Katz paradigm is a well-known logical trap that, if sprung, would threaten to erode privacy entirely. The trap is simple: If a person knows she is being watched, she cannot expect to be not 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. To fall into this trap is to commit an is-ought fallacy, conflating the factual expectation in the objective test with a normative one, for which a better phrase would be a “privacy interest.” Call the new requirement “objectively reasonable subjectivity.” The two part test should instead be: 1) does a person have a right to privacy in this instance

76 “Justice Harlan himself later expressed second thoughts” about the word “expectation,” due to the circularity problem. Amsterdam, supra note 71, at 384 (1974).


78 See, e.g., Rubenfeld, supra note 75, at 106 & n.23 (collecting sources); see also Amsterdam, supra note 71, at 384 (“An actual, subjective expectation of privacy ... can neither add to, nor can its absence detract from, an individual’s claim to fourth amendment protection. If it could, the government could diminish each person’s subjective expectation of privacy merely by announcing half-hourly on television that ... we were all forthwith being placed under comprehensive electronic surveillance.”).
and has he or she 2) exercised it? This structure is similar to reasoning about waiver of rights in other areas of law. First the law asks whether a person has a certain right and then whether he or she has asserted that right or waived it.

The Court’s approach to this has been unforgiving, treating any risk at all of exposure as de facto exposure.\textsuperscript{79} For example, in both \textit{California v. Ciraolo}\textsuperscript{80} and \textit{Florida v. Riley},\textsuperscript{81} the Court ruled that because someone could possibly rent a plane and fly over property, it was unreasonable to expect that the activities on the property were hidden, and thus the privacy interest did not exist. The Court returned to this doctrine in \textit{Kyllo v. United States}, implying that once a privacy-defeating technology becomes commonplace, people cannot reasonably expect that it will not be used, and therefore will not have a privacy expectation.\textsuperscript{82}

The blending of the objective and subjective into “objectively reasonable subjectiveity” could not have occurred if the two concepts were more distinctly analyzed, rather than part of a single inquiry—that of a “reasonable expectation of privacy.” Contextual integrity is a useful tool here, as it implements this twofold requirement as two separate steps. The objective inquiry is the framework analysis. In the framework analysis, the theory is asking, “Does society recognize an expectation of privacy here?” It answers the question by describing the expected information flows, which are based on informational norms—that is, societal rules about information. The subjective expectation, on the other hand, is folded into the violation inquiry. 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 something and yelling it across the room.

Returning to the \textit{Terry} example, recall that the transmission principle was precisely this: control. Terry was in control of the information about what he was carrying, except if the police had a warrant or a warrant exception. This means that if the weapon were displayed openly, the defendant would have exercised the control by choosing to openly expose the information. Therefore, a police officer seeing it would not have been a violation of an informational norm. However, because Terry exercised control to hide the weapon, the police officer’s search was a violation. This

\textsuperscript{79} Colb, \textit{supra} note 35, at 121-22.
\textsuperscript{80} 476 U.S. 207 (1986).
\textsuperscript{81} 488 U.S. 445 (1989).
\textsuperscript{82} 533 U.S. 27, 34 (2001)(“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.”).
is Justice Harlan’s subjective formulation. His formulation, however, only covers cases in which control is the relevant transmission principle, while contextual integrity provides a more general framework.\textsuperscript{83} Moreover, because the framework analysis and violation inquiry are conducted separately in a contextual integrity analysis, the kind of conflation that leads to the circularity in Katz does not occur.

A related issue worth expressed most recently by Justice Alito in his concurrence in United States v. Jones:

The Katz expectation-of-privacy test . . . is not without its own difficulties. It involves a degree of circularity. . . [and it] rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. . . . [E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.\textsuperscript{84}

Worrying that people will reconcile themselves to an undesired order, Justice Alito conflated objectively reasonable subjectivity with the issue of changing cultural privacy norms. Changes in privacy mores are not new and are not solely caused by technology; American society has become less formal and thus more open for decades. While there has been a technology-aided acceleration of that change, the frequent privacy scandals in the news demonstrate that the capability of technology to invade privacy is changing much faster than our willingness to allow it do so. So, while norm evolution may erode privacy protections similarly to objectively reasonable subjectivity, the erosion would occur only in step with society’s desire for privacy. If as a society, we conclude that we do not desire privacy, unlikely a result as that seems, than that is arguably the right result for the Fourth Amendment as well.

B. State Action and the Divergent Meanings of “Search”

As any confused law student in Criminal Procedure can tell you, current doctrine defines a “search” in a way that is completely at odds with the English language. If police are riding down the street in a patrol car looking for a suspect, English speakers might naturally say that the police

\textsuperscript{83} See supra note 46 and accompanying text.

are “searching,” but the Fourth Amendment disagrees.\textsuperscript{85} This linguistic shift 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.”\textsuperscript{86} The plain view doctrine makes sense, but it is only a restatement of state action doctrine. If the police are not looking for anything and happen to witness a crime or find evidence, then the Fourth Amendment is not implicated \textit{because there is no state action}.\textsuperscript{87} Similarly, if a co-conspirator decides to become an informant of his own volition, there is no state action, and the Fourth Amendment is not implicated. But often where there is police action, either to look for evidence or to turn a suspect into an informant,\textsuperscript{88} current doctrine still says there was no “search.” Thus entire classes of actions are eliminated from the Fourth Amendment’s purview based on reasoning that should only eliminate situations that lack state action.

It has become dogma that police cannot have \textit{less} access to information than the average person. State action, however, doctrine serves the general purpose of limiting government action, often where citizens are permitted to take the same action. 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.\textsuperscript{89} Thus if search amounts to state action, there is no reason that police should have equal access to non-government actors. Obscuring these limitations is the prime effect of the linguistic abuse of the word “search” in current doctrine. Because the \textit{Katz} test looks for an expectation of privacy that society is prepared to accept as reasonable, the doctrine should conform to how society understands the relevant terms. The category differences between natural language and legal doctrine turns the term “search” into a set of arbitrary doctrinal bins that become self-justifying as future cases look to precedent, rather than being justified in relation to the concepts on which they were originally based.

\textsuperscript{85} Probably the most obvious examples of this phenomenon are \textit{California v. Ciraolo}, 476 U.S. 207 (1986), and \textit{Florida v. Riley}, 488 U.S. 445 (1989), where police flew a plane and helicopter respectively over the defendants’ land, and yet it was not considered a search.


\textsuperscript{87} This is different than the case when the police are looking for one thing and inadvertently find something else, as discussed in \textit{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.

\textsuperscript{88} \textit{Hoffa v. United States}, 385 U.S. 293 (1966).

The approach in this Article separates the concepts of “search” and “reasonable expectation of privacy,” with the former simply meaning state action and the latter defined by contextual integrity, with both required to find a Fourth Amendment violation. This move is consistent with Katz in its original form, which would have presumed both a state action requirement and some sensible definition of a reasonable expectation of privacy. Figure 1 explains the analytical structure change. Paring back the definition of search in this way would render a great deal more police activities 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. So, 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. In the case that the police go to the suspect’s house with a warrant, that is similarly a reasonable search because it comports with transmission principles—specifically, having a valid warrant. Thus a warrant is just one possible element of determining a reasonable search.

The focus on state action here is not meant to suggest that state action is missing from the current doctrine. Undoubtedly, if someone tried to sue his neighbor for a Fourth Amendment violation, he would be laughed out of court. Rather, state action is actually double counted: once in the normal way, and once again as plain view doctrine, which is in turn only part of a larger search doctrine. Separating search from reasonable expectation of privacy realigns the two applications of state action into one consideration again.
Analytical Placement of Key Questions in Current and Proposed Search Doctrines

Current Fourth Amendment Search Doctrine

Was it a search? (Step 1)

State Action?

Reasonable expectation of privacy?

Is there a warrant or established exception?

Is the search reasonable? (Step 2)

Should there be a new warrant exception?

Is the violation or non-violation normatively preferred? (Normative Layer)

Contextual Integrity-Based Search Doctrine

Was there a search? (Step 1)

State Action Doctrine?

Is there a prima facie contextual integrity violation? (Descriptive Layer)

Figure 1
The second difference between the analytical structure of contextual integrity and current doctrine is that warrants and warrant exceptions get encoded as part of transmission principles, seen in Figure 1 as part of the descriptive analysis. Under this theory, it cannot be determined whether a reasonable expectation of privacy was violated without the information about a warrant; it is all one step. Recall, though, that the text of the Fourth Amendment never mentions “searches” as a standalone concept. Rather, it only addresses “unreasonable searches.” Thus, a single query about whether a police action was an unreasonable search is truer to the text as well.

C. 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. When the two questions of whether there is or ought to be a warrant exception in a given case are asked simultaneously, it is very easy to grant new exceptions that are similar to old ones, without necessarily thinking of the new part as really new. This is why the doctrine has slowly crept along allowing more and more things not to be subject to it. Contextual integrity, however, shunts the inquiry about current state to the descriptive analysis, so only the normative question remains: Should the outcome of the descriptive layer stand?

Contextual integrity also has the benefit of putting the values on the table – contextual as well as general values – and basing the inquiry on those values. However, identification of the values at stake is as far as the theory can go. Normative judgment cannot be escaped, but identifying the values correctly makes it easier to gather empirical evidence of people’s views, or to have meaningful debates anchored in some other source of ethical reasoning. In the end, the debates inherently remain arguments about what kind of society we want to live in. These principles are always in the background, but the contextual integrity approach brings the principles and values in question to the foreground and requires that they be sorted out.

III. Search Doctrine As Contextual Integrity

The last section described in the abstract how the contextual integrity approach solves some of the difficulties with the current interpretation of the Katz test. This section analyzes several cases to illustrate both how to use the theory in a Fourth Amendment case and what

---

90 U.S. CONST., amend IV.
91 [CITE]
92 See, e.g., Slobogin & Schumacher, supra note Error! Bookmark not defined..
the doctrine would look like with contextual integrity as the operational theory. The selection of cases and doctrines is not by any means meant to be exhaustive, but rather is intended to show how contextual integrity either matches or changes some of the more basic parts of search doctrine. The cases are grouped by individual doctrine or idea that animates them – third party doctrine, privacy in public, emanations, and roving wiretaps.

There are two types of cases for which current doctrine and contextual integrity are in clear agreement. They 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 a state action requirement, present in both versions of the theory. Unjustified police entry also violates both standard Fourth Amendment doctrine and contextual integrity for essentially the same reason. As a matter of current law, it is a relatively simple conclusion, as courts have said that the “home” is so quintessentially a private place that physical intrusion even by a “fraction of an inch” is too much.93 Contextual integrity would instead say that the home is a specific social context and as against the police, the contents of ones’ home are subject to the transmission principle of “control by the resident, except if the police have a warrant or justification.” Thus the unjustified entry is a prima facie violation, and the discussion moves to the normative layer. Because 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, the normative answer is 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.94

The discussion in this Part focuses on more difficult cases and doctrines: third party doctrine,95 including cases involving information released to third parties96 and the use of informants,97 cases expressing the

---

94 See infra Part IV.A.
95 Third party doctrine, as commonly understood, consists of two separate sets of cases: cases involving information released to a third party and informant cases. Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 566 (2009). The doctrines are considered separately and should not be confused, despite their similarities.
96 See, e.g. United States v. Miller, 425 U.S. 435, 443 (“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...
idea of “no privacy in public,” emanations and dog sniffs, all of which are dismissed as “not a search” under current doctrine. There is also a short section on roving wiretaps. According to the theory presented here, the threshold issue is not whether there was a “search,” but whether the action in question is a violation of contextual integrity as a descriptive matter. Often, it is, and sometimes, the question cannot easily be answered without more information, such as empirical observations about society’s norms. 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 not able to do lacking a context-based theory. The conclusion in this section often echo the critiques of many other Fourth Amendment scholars writing, for example, about courts’ equation of a possibility of exposure with probability of exposure, and that in turn, with actual exposure. Contextual integrity is a very different looking analysis, but its results line up with many mainstream critiques of the current doctrine. 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. Originating from two cases, United States v. Miller and Smith v. Maryland, the doctrine states that there is no expectation of privacy in information knowingly disclosed to a third party. The Court ruled in Miller that there is no Fourth Amendment interest in bank records, because the records have been exposed to someone (a bank), and thus they are no longer private. In Smith, there was no interest in the phone numbers a person dialed because the records have been exposed to someone (a bank), and thus they are no longer private. In Smith, there was no interest in the phone numbers a person dialed because the records have been exposed to someone (a bank), and thus they are no longer private. In Smith, there was no interest in the phone numbers a person dialed because the records have been exposed to someone (a bank), and thus they are no longer private. In Smith, there was no interest in the phone numbers a person dialed because the records have been exposed to someone (a bank), and thus they are no longer private.

---

98 See, e.g., United States v. Knotts, 460 U.S. 276, 281 (1983) (“A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”).
99 Kyllo 533 U.S. 27.
100 E.g., Illinois v Caballes, 543 U.S. 405 (2005).
101 See Slobogin & Schumacher, supra note Error! Bookmark not defined.. supra note 35, at 121-123.
102 See, e.g., Colb, supra note 95, at 563 (“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.”)
103 Kerr, supra note 95, at 563.
106 Kerr, supra note 95, at 563.
to the telephone company. Criticisms of these decisions abound, and the doctrine even seems to be falling into disfavor with the Court. Nonetheless the doctrine is frequently relied on by law enforcement.

This is one of the simpler doctrines to examine with contextual integrity, as an in-depth look at Miller will demonstrate. The facts of Miller are as follows: Mitch Miller was suspected of operating an illicit distillery, and as part of their investigation, agents from Alcohol, Tobacco, and Firearms issued a subpoena for “all records of accounts, i.e., savings, checking, loan or otherwise, in the name of Mr. Mitch Miller.” The bank then, without telling Miller about the subpoena, gave all the records to the police, and eventually, on the strength of those records, Miller was convicted.

At trial, Miller moved to suppress the records, and the district court denied the motion. 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. Eventually the Supreme Court reinstated the district court’s decision. 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,” but the Court rejected that argument, saying that “in Katz the Court also stressed that ‘[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.’”

Under contextual integrity analysis, that exchange is the crux of the matter. The analysis begins with the framework. Who are the agents (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 attributes are financial information – the checks and deposits named in the motion. Finally, consider the

---

107 Strandburg, supra note 23, at 103 n.10 (collecting critical writings).
108 Id. at 104 (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.”)
109 Miller, 425 U.S. at 437. The subpoena was cited as “allegedly defective,” but the Court specifically ruled irrespective of the subpoena’s validity. Id. at 440.
110 Id. at 436.
111 Id. at 437.
112 Id.
113 Id. at 442.
114 The bank certainly also had contact information, such as name, phone number, and address, but most likely a different transmission principle guides those parts. Here the state convicted on the strength of the bank records, not because the police used the contact information, so that is the relevant information to consider.
transmission principle. Banking customers give checking information to banks that they would not want the public to know; people generally do not share even bank account numbers with very many others, let alone balances, payments, or deposits. Customers do so because the bank needs to track that information simply to provide its essential services. Many people would be outraged at the knowledge that their information has been passed on to others, to the point of switching banks or filing lawsuits even for accidental sharing of information.\textsuperscript{115} This is a good piece of evidence for a transmission principle.\textsuperscript{116} As always, there will be the additional element that with a warrant or warrant exception, the police may have access to this information. 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.

The framework established that there was a reasonable expectation of privacy in this type of information flowing between these agents. 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.\textsuperscript{117} 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 new norm? At the margins, surely, money would flow less freely in society, and people would be more prone to stuff money under a mattress with this new norm than without it, but the banking system did not collapse when this case was decided in 1976, so perhaps that point is not good enough. The normative analysis has to balance the harm to the banking context, participation in which we rely for financial autonomy via savings and home ownership, and which is necessary for investment in our market-driven society, against the aid to law enforcement of warrantless access to the records. 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

\textsuperscript{115} Sasha Romanosky, David Hoffman & Alessandro Acquisti, \textit{Empirical Analysis of Data Breach Litigation}, at 3 (SSRN Working Paper Series), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461. (“[T]he odds of a firm being sued from improperly disposing data are . . . 6 times greater when the data breach involved the loss of financial information.”)

\textsuperscript{116} See supra Part I.A (“People’s indignation, anxiety, fear, anger, and outrage over a privacy violation is evidence that an informational norm has been breached, and protest and resistance often follow.”).

\textsuperscript{117} If the bank had noticed that the accounts were fishy on their own accord and handed over the documents, there would have been a contextual integrity violation, but no Fourth Amendment violation because there was no state action.
Amendment privacy?" Perhaps, but it seems doubtful. Regardless of the specific answer, though, 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 point in the case was that Mitch Miller gave the documents to the bank “for a limited purpose.” After balancing the interests, a court could have concluded in a context-conscious ruling that banking documents are too important for law enforcement compared the limited harm to the banking system if consistently disclosed. A context-conscious ruling could not, however, have created the third-party doctrine as a blanket rule.

In fact, the Court was not completely unaware of the importance of context. Four more statements came after the announcement of the third-party doctrine as a general proposition, at least the first and third of which betray such an awareness:

(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 proceedings.”

(4) The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. United States v. White, 401 U.S. 745, 751-752, 91 S.Ct. 1122, 1125-1126, 28 L.Ed.2d 453, 458-459 (1971). 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.

Statement (1) suggests that confidential communications would be entitled to privacy protections, but that the documents in question were just

---

120 Id. at 442-43.
“negotiable instruments,” ignoring the sensitive nature of much of the included information. The Court was suggesting a requirement of explicit confidentiality in privacy protections, which seems at odds with the concept a “reasonable expectation of privacy”—in effect saying it is unreasonable to expect privacy unless agreed upon first. This is only true in situations where it is otherwise unreasonable to expect privacy, and thus the reasoning is completely circular. Statement (1), with its awareness of context, seems inconsistent with the third-party rule stated just a few sentences earlier.

Statement (2) is definitely true, implicitly equates exposure to the bank for limited purposes and exposure to the public at large. The voluntariness of the disclosure is conceded, but it was not at issue. The issue instead was the difference between exposure to a bank and the public at large, which the Court simply missed.

Statement (3) is simply false or at least, unsupported. The statement claims that Congress, by requiring preservation of documents, foresaw and permitted a movement of information from one context to another. While it is true that Congress must have foreseen it, the statement does not support the idea that Congress has authorized it without any form of process.

Statement (4) connects the information-based third-party doctrine with precedent from the cases involving informants. The Court had previously said that a person takes a risk when disclosing information to someone who might potentially be an informant.\textsuperscript{121} However, to apply the same reasoning to an institution known to be regulated, and on which society depends\textsuperscript{122} for confidentiality, betrays an insensitivity to context that would not have been possible under a contextual analysis. As a normative matter, the reasoning in the informant cases is that people should be careful choosing their friends,\textsuperscript{123} but to place those same conditions on an institution such as a bank is inconsistent with societal norms for that context.

The dissent demonstrated sensitivity to context, arguing that the privacy at stake was that of Miller, not that of the bank:

\textit{[T]he voluntary relinquishment of [ ] records by the bank at the request of the police does not constitute a valid consent by this petitioner. . . . It is not the right of privacy of the bank but of the petitioner which is at issue, and thus it would be untenable to conclude that the bank, a neutral entity with no significant interest in the matter, may validly consent to an invasion of its}

\textsuperscript{121} \textit{Id.} at 440 (citing \textit{Hoffa v. United States,} 385 U.S. 293, 302 (1966)).

\textsuperscript{122} \textit{Id.} at 451 (Brennan, J., dissenting)(“[I]t is impossible to participate in the economic life of contemporary society without maintaining a bank account.”)

\textsuperscript{123} \textit{See infra} Part III.B.
depositors' rights.\textsuperscript{124}

Under the contextual analysis, consent of the subject was a part of the relevant transmission principle. Here, as the dissent observed, there was no consent in the transfer of information. Further, the informant cases on which the Court relied all required the subject’s consent to the third party receiving the information, specifically in the form of the defendant spilling the beans himself. In contextual integrity terms, the transmission principle would say that the subject has control over this information, so if the subject were also the sender, the transmission principle would no longer involve confidentiality, but rather control, and thus the informant cases are quite different in that regard.

\textit{Smith v. Maryland}\textsuperscript{125} has the same problems as \textit{Miller}. The Court ruled that because the phone numbers are relayed to the phone company they are no longer private. Just like in \textit{Miller}, this equates the employees of the phone company, in a specific, limited relationship with the defendants, with the public at large. Normatively, the Court should have been asking if it is in society’s interest to condition telephone use on the waiver of Fourth Amendment rights, much as it so 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\textsuperscript{126}) and perhaps that is why the doctrine may be falling by the wayside.\textsuperscript{127}

\textbf{B. Informants and “Pretend Friends”}

Some of the flaws in the third-party doctrine stem from its reliance on the equally flawed informant cases.\textsuperscript{128} In these cases, a police officer gathers information either by going undercover and becoming a “pretend friend”\textsuperscript{129} 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 amendment affords no protection to ‘a wrongdoer's misplaced belief that a person to whom he

\begin{footnotes}
\item [124] Id. at 450 (ellipses in original).
\item [125] 442 U.S. 735 (1979).
\item [127] See supra note 108.
\item [128] Miller, 425 U.S. at 440 (relying on Hoffa v. United States, 385 U.S. 293, 302 (1966)).
\item [129] Colb, supra note 35, at 139.
\end{footnotes}
voluntarily confides his wrongdoing will not reveal it.’”\footnote{United States v. White, 401 U.S. 745, 748 (1971) (quoting Hoffa, 385 U.S. at 302 (1966)).} The Court, however, 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 convince said confidant to turn, perhaps but not necessarily in exchange for immunity, and, 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. While the Supreme Court’s stance is that none of these scenarios counts as a search, the information flow changes significantly in each one. The first scenario, however, requires no action at all by the police, and thus it would not qualify as a search under either theory. This is also why the first scenario never shows up in the governing cases. The second and third scenarios do contain state action, and thus the information flows need to be examined.

In \textit{Hoffa v. United States}, the police convinced an incarcerated former associate of Jimmy Hoffa’s to become an informant in exchange for dropping the charges against him.\footnote{385 U.S. at 298.} Hoffa then told his former associate incriminating information, the associate reported it to the police, and Hoffa was convicted on that information. There are two information flows here: Hoffa to associate and associate to police. The first is not new – Hoffa and the associate shared information constantly; it is the second flow that raises concerns. Here Hoffa is the subject, the associate the sender, and the police the receivers. The attribute is incriminating information, specifically, conversations about jury tampering. The relevant transmission principle would be that a person doesn’t rat on his friends or associates. As to the police, the principle is \textit{withhold}.

In \textit{Lewis v. United States},\footnote{385 U.S. 206 (1966).} a police officer misrepresented his intent as someone who had an interest in buying drugs – the 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. However, if someone represents himself as a part of one context, he is bound by its rules at a minimum. Someone, for example, who pretends to be a doctor, certainly does not get to take \textit{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 the receiver. The attribute is a desire to sell drugs. The transmission principle is that a
potential buyer shares in that information freely, but it is withheld from 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 flows changed. The normative layer then asks whether indiscriminate undercover police work is worth the cost to the fabric of social relationship in society.\textsuperscript{133} At the margins, if people believe that neighbors, friends, employers or clients could be reporting to the police, the relationships will suffer. If people believe 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 police radar. The fact 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 the recent revelation that the NYPD infiltrated Muslim Student Associations throughout the tri-state area,\textsuperscript{134} based on the strange rationale that police merely go where there are “allegations.”\textsuperscript{135} The result, predictably enough, is that students in these groups now avoid talking about politically sensitive subjects, if they can get past the pressure from their families urging them not to join at all.\textsuperscript{136} If the rule is instead that police at least must have 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.\textsuperscript{137} This is the worry behind the warrant requirement in every other situation as well.

The winning arguments in the real cases took the form of an assumption of the risk rationale: people should be careful whom they trust, and if confidants turn on someone, the information is fair game. This

\begin{flushright}
\textsuperscript{133} Here we are merely discussing \textit{suspicionless} undercover work, which is what the Court ruled permissible.
\textsuperscript{134} Chris Hawley, \textit{NYPD Spied On Muslim Students At Yale, All Over The Northeast}, HUFFINGTON POST (Feb. 20, 2012), http://www.huffingtonpost.com/2012/02/21/nypd-spied-on-muslim-stud_n_1290544.html.
\textsuperscript{137} Such a rule would not “severely hamper undercover investigations,” as Orin Kerr fears, Orin S. Kerr, \textit{The Case for the Third-Party Doctrine}, 107 MICH L. REV. 561, 568 (2008), because the required level of suspicion can differ with specific context. Beyond the dividing line of \textit{some} suspicion or \textit{none}, the specific level of suspicion required in each case is beyond the scope of this Article – all we are saying it that \textit{some} should be required.
\end{flushright}
rationale, like the extension of plain view doctrine discussed earlier, ignores the state action differences between the cases, and does not support the outcomes it is meant to. There is a substantive difference between spontaneous treachery and police coercing or even cajoling someone into betraying his friend, just as there is a difference between someone openly displaying guns on the street and the police finding them in a frisk. 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 they do not trust.\(^\text{138}\) The suppression of police action as a data point turns a Fourth Amendment question into victim-blaming.\(^\text{139}\)

The Court can be forgiven for deciding \textit{Hoffa} and \textit{Lewis} the way it did, because both came a year before \textit{Katz} made a “reasonable expectation of privacy” the touchstone for Fourth Amendment search. However, four years later, the Court decided \textit{United States v. White}, extending the holding of \textit{Hoffa} to include situations where the informant was wearing a wire,\(^\text{140}\) and declaring that \textit{Katz} left informant doctrine unchanged.\(^\text{141}\) This is odd, when one considers that both cases involved a hidden electronic device relaying information back to the police.\(^\text{142}\) At least the similarities warranted more than a cursory dismissal, but in the end the court stuck with the “traitor detector” rationale of the pre-\textit{Katz} cases. The Court then reasoned that there was no difference between the informant hearing the information then telling the police and it being relayed electronically in the first place.\(^\text{143}\) 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.\(^\text{144}\)

\(^{138}\) Colb, supra note 35, at 142. To borrow Professor Colb’s analogy whether a person has a home alarm system or not perhaps makes it more or less likely that their 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 they were being careful enough.

\(^{139}\) \textit{Id.} (analogizing to a burglary of a house without an alarm system); \textit{see also} Amsterdam, supra note 71, at 406-07 (analogizing to the inherent risk of parking a car in Greenwich Village, New York).

\(^{140}\) 401 U.S. 745 (1971).

\(^{141}\) \textit{Id.} at 749.

\(^{142}\) Colb, supra note 35, at 141.

\(^{143}\) \textit{White}, 401 U.S. at 752.

\(^{144}\) \textit{See, e.g.,} Cal. Penal Code §§ 631, 632; Mass. Ann. Laws ch. 272, § 99. These laws are not the only indication of the information flow disruption, and accordingly, the
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. The germ of this idea originates in *Katz*: “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” The Court has built a great deal of doctrine upon this idea, though *United States v. Jones* demonstrated that at least five Justices might be inclined to reconsider. *United States v. Knotts* is a prominent example of this doctrine at work:

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. The Court said later:

[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.

The rationale is brought sharply into focus by contrast with *United States v. Karo*, a subsequent case presenting quite similar facts. The operative difference between the two is that in *Karo*, unlike in *Knotts*, the fact that not all states have two-way consent laws (or that several have carve-outs for law enforcement, see e.g., 18 Pa. Cons. Stat. § 5704(2)) does not demonstrate a definitive lack of information flow disruption.

---

145 NISSENBAUM, supra note 17, at 113.
147 132 S.Ct. 945 (2012).
149 *Id.* at 284.
police continued to track the person inside a home.\textsuperscript{151} Based on that difference alone, the Court in \textit{Karo} found a Fourth Amendment violation.\textsuperscript{152} While it certainly is arguable that a person expects more privacy in the home, these cases create a hard-line distinction. Moreover, these two cases ignore the observation from \textit{Katz} that the Fourth Amendment “protects people, not places.”\textsuperscript{153}

Needless to say, under the contextual integrity approach, the fact patterns in these two cases are analyzed differently than the Court’s approach. \textit{Knotts} is a more complex case, with more information flows, so it will illuminate more about the theory’s operation. The facts of \textit{Knotts} are as follows: Minnesota police suspected that one co-defendant, Armstrong, was purchasing chloroform as part of an illegal drug manufacturing operation.\textsuperscript{154} The police then convinced the seller of the chloroform to insert a “beeper” into one of the purchased containers.\textsuperscript{155} 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.”\textsuperscript{156} The police used the beeper to follow Armstrong from the chemical company to the cabin of a second defendant and the respondent, Knotts. 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.\textsuperscript{157}

\textit{Knotts} contains two different relevant information flows within a few overlapping contexts and relationships. The problem can be simplified by 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

\begin{itemize}
\item \textsuperscript{151} \textit{Id.} at 714.
\item \textsuperscript{152} \textit{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.”)
\item \textsuperscript{153} \textit{Katz} v. United States, 389 U.S. 347, 351 (1967). The home, however, is still worth protection as a social context as well as a place. The rationale just needs to change, and with it the hard line approach. See \textit{infra} part IV.D
\item \textsuperscript{154} \textit{Knotts}, 460 U.S. at 278.
\item \textsuperscript{155} \textit{Id.} This should immediately call to mind the informant cases, which we shall soon see are quite related to \textit{Knotts} in ways the Court could not have explored given the shape of its jurisprudence.
\item \textsuperscript{156} \textit{Id.} at 277.
\item \textsuperscript{157} \textit{Id.} at 279.
\end{itemize}
broadly, or specifically to the police, it would have violated the
transmission principle governing their relationship. Because that is the case,
where control is a part of the transmission principle, it is reasonable to
assume that they would have chosen to exercise the same level of control,
and thus they 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
broadcast the defendant’s whereabouts. The first concerns the relationship
between the police as receiver and the defendant as subject and sender of
his own whereabouts. 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.

Examining the first information flow – the police gathering location
information by following a suspect – it is one of the situations in which
police are not simply a standard third party plus a badge. The reasons to be
apprehensive about being followed by a stranger are different than those
that might apply to 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 absence of individualized suspicion, as without any suspicion it is
probably for some other illicit motive, such as improper profiling. However,
we do expect police to (literally) follow leads when necessary. Thus, while
a prohibition on police following is not the informational norm, it does not
follow automatically that there should be no limits.158 This error is laid plain
by the holding of Karo, which said the police were not permitted to follow
the defendant once he was inside a house. 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 (in the absence of administrability
concerns);159 the more intrusive the following, the higher level of suspicion
and procedural protections that should be required.160 This is at least part of
the intuition behind the concern about prolonged surveillance in Jones.161

158 Contra id. at 281-82.
159 See supra note 71; see also infra notes 340-345 and accompanying text (discussing
the proportionality principle).
160 [CITE Slobogin’s new paper for legislating mosaic theory as an sample graded
proposal]
161 United States v. Jones, 132 S.Ct. 945, 955 (Sotomayor, J., concurring), 964 (Alito,
J., concurring).
Lacking empirical data about society’s views on permissible police conduct, the exact transmission principle is unclear. Thus the violation inquiry will also 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\(^{162}\) nor continued use once defendant was inside a private home.\(^{163}\) So leaving aside the technology for the moment (the specific effects of technology are discussed in Part V), this means that the officer followed the suspect without a warrant, but probably with some level of suspicion and for a only moderate length of time. Given this middling information, it is impossible to say here whether the first information flow violated an informational norm.

The second information flow, however, did violate a norm. The agents are identified above, the attribute of interest is the defendant’s whereabouts, and the relevant transmission principles are those governing the market context.\(^{164}\) 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. That information is subject to an expectation of confidentiality; if customers discovered a store was selling their credit card information to third parties, they would soon have many fewer customers. Transmission principles about other kinds of

\(^{162}\) *Knotts*, 460 at 283.

\(^{163}\) *Id* at 284.

\(^{164}\) It is certainly a valid position that the relevant context here is more limited to “the market for dangerous chemicals.” Because certain chemicals are inherently dangerous, or even perhaps because they are used to manufacture drugs, it might be inherent to the chemical sale context that information may be given to the police if there is reason for suspicion.

Defining the specific boundaries of the context is partly a normative task, which itself defines the relevant values and thus the transmission principles. *See supra* note 50 and accompanying text. In a full analysis, all the possibilities would have to be run descriptively, and then the normatively layer would be debated, and in it the appropriate context defined, choosing the correct descriptive scenario. The process is thus iterative in this way.

Before getting to the normative questions, though, we can at least say here that the appropriate context is one of these two reasonable possibilities. Further, with respect to the particular information at issue – the defendant’s *whereabouts* – the transmission principle is likely the same. 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 someone would like to define contexts. They should continue to be useful social contexts to have any useful meaning, but that line is certainly fuzzy. *See NISSENBAUM, supra* note 17, at 223.
information are different between a store online today and a physical store, such as what exactly a customer examines and for how long; if a store employee followed a customer with a notepad, it would be discomfiting, but this is par for the course online. However, with respect to the whereabouts of the customer after leaving the store, that information is in complete control of the customer. He may tell the store owner he is going fishing right after leaving the store, but if he does not mention anything, contextual integrity does not permit the store owner to follow him to the lake. The control principle acts both against the seller’s awareness of the whereabouts and any third party that the seller might inform.

Now onto the violation inquiry. Because the relevant information is not part of sale, but is post-sale location information, it is subject to the principle of control by the subject. Whether the seller obtained it himself or enabled any third-party, including the police, to obtain it, informational norms were violated. Because the seller’s violation was done at the behest of the police, it implicates the Fourth Amendment as well. The normative analysis, then, needs to determine whether the police’s ability to get a third party to change this information flow is preferred over the status quo. Consider the market context. If people knew that a seller was more likely than other to cooperate with police, he would not use that seller, and if all sellers did, he might think twice about buying even harmless things. There are certainly people who refuse to shop online despite the enormous convenience because they are constantly being tracked, and if someone were to track a customer in a physical store, the customer would call security. On the other hand, the police must be able to track suspects, and a warrant requirement slows that process. In the end it comes to a balancing question.

Interestingly, under this construction, Knotts has similarities to an informant case, due to the use of a third party to redirect the information. Because the court dismissed it based on the “no privacy on public roads” rationale, considering only the act of following, the case did not seem similar before. Of course, the informant cases are similar to informational third party doctrine, so they’re all connected. The same normative arguments about whether society wants to condition banking or social relationships on the potential involvement of the police apply here to the market context, counseling against giving the police carte blanche to use third parties for tracking.

A slightly different example of the “no privacy in public” rationale is the automobile exception to the warrant requirement. Because it is a warrant exception, it is not actually a question asked in the first half of the Fourth Amendment analysis, and so in these cases, a search occurred under current law. The automobile exception is premised on three different
rationales: 1) the exigency created by the fact that the vehicles can move quickly away, 2) that police interact with vehicles much more often than homes, and 3) “the obviously public nature of automobile travel.”\textsuperscript{165} The first is not novel – exigency is a familiar, self-contained warrant exception – but the other two rationales are. The second is based partly on the publicity of the vehicle; constant contact means that the police are able to stop it on the road or see into it.\textsuperscript{166} Meanwhile, the third rationale is explicitly the privacy in public question. In a later case, the Court ruled that a motor home could be searched under the automobile exception.\textsuperscript{167} The three dissenting justices in that case argued that a parked motor home was like a home, but so pervasive is the “no privacy in public” rationale that the dissenting justices said “warrantless searches of motor homes are [] reasonable when the motor home is traveling on the public streets or highways.”\textsuperscript{168}

Automobiles arguably make up their own context, perhaps more accurately considered “commuting.” The sense of serenity and privacy in a person’s car is similar to how a person might view his home, but as the Court acknowledged, slightly less restrictive. A guest has to be invited into the car and would not go into the glove compartment snooping around, just like a home. However, there is a lot more interaction with police in a car, as officers can stop drivers more easily than search a home and they can see a greater part of the car through its windows than they can a home. The second rationale seems to support the idea of a context similar to the home, but slightly less private, without needing to resort to the “no privacy in public” idea. Indeed, the latest word on the automobiles, \textit{Arizona v. Gant}, held that after the driver of an automobile is arrested and secured, a search of an automobile is impermissible under the “search incident to arrest” warrant exception, unless there is probable cause to suspect that evidence will be found.\textsuperscript{169} This confirms that the automobile exception still contains some privacy protection, despite being in public. \textit{Gant} might be another data point that the Court is starting to reconsider its reliance on the “in public” argument.

\textbf{D. Emanations}

\begin{itemize}
\item \textsuperscript{165} South Dakota v. Opperman, 428 U.S. 364, 367-68 (1976).
\item \textsuperscript{166} \textit{Id.} The second rationale also deals with registration and licensing. Because the car is so often seen by the authorities, one simply cannot expect privacy in it. So not only is the automobile inspection based in privacy in public, but also the standard is-ought conflation in the \textit{Katz} test.
\item \textsuperscript{167} California v. Carney, 471 U.S. 386 (1985).
\item \textsuperscript{168} \textit{Id.}
\item \textsuperscript{169} Arizona v. Gant, 556 U.S. 332 (2009)
\end{itemize}
Cases about emanations are different than the ones discussed so far. All people constantly emanate light, heat, smells, sounds and other information, including DNA. These emanations contain a great deal of information about a person, and technology is enabling the police to glean more and more from these involuntary excretions. For the most part, search doctrine has not considered emanations as a class of contexts, but has treated them slightly differently depending on the case. For example, using dogs to sniff for drugs is not a search. Dogs, according to the Court, are a sui generis case because they only give the limited information about whether or not illicit drugs are present. On the other hand, the Court treated emanated heat very differently in *Kyllo v. United States*, 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.

The fact that the heat emanated into public did not matter, because the police used technology that was not generally available to the public to detect the emanation.

Emanations can be described by information flows just like anything else. In people day-to-day lives, people expect that others can see them walking around and can hear some level of what they do. People naturally disguise themselves if they do not want to be recognized and keep their voices down if they do not want to be overheard. These observations are at the heart of the Court’s complaint that police need not “avert their eyes,” and here the Court is absolutely right. However, the typical information flows with respect to emanations rely on several other assumptions, such as practical obscurity. When people walk down the street, they do not expect to be recorded, except possibly by the passing tourist or artist, who is not recording a person because of his identity, but rather as part of the scenery. People expect the other pedestrians to forget them because each of us is irrelevant to passersby. People have conservations in cafes expecting that no one cares what they are saying and thus will not retain it. 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

---

173 *Id.* 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.
175 *Id.* at 35-36.
information.

Part of society’s reasonable expectation, then, is that information flows will be limited by human capabilities. Humans have a limited degree of perception. If people speak at normal volumes inside homes, they reasonably expect not to be overheard because humans cannot hear through the walls. Of course, people in apartments with thin walls know differently and expect differently. However, when the police listen in, either with their ear to the door or a microphone, they are violating that expectation. The same goes for smells. When people smoke marijuana, they generally understand that people nearby can smell it, and they sometimes take precautions such as a wet towel under the door. If the police smelled the marijuana, they would not be required to ignore their noses, but that is different than employing a dog to smell what would otherwise go undetected. Sensory information is also bounded in time just as much as other limits of perception, and recording makes it possible to witness emanations 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 other information flow disruptions. Human memory is faulty, and juries feel differently about recordings than live testimony from witnesses. All 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 as every other information flow.

In this light, the difference between Caballes and Kyllo is hard to reconcile. In both, police are taking an action that goes beyond merely unwittingly noticing that a certain emanation occurs. If the police in Kyllo had walked by and felt the heat or observed snowmelt, the case would have

---

177 This point seems to imply that those with thin walls have lesser Fourth Amendment rights than those with fuller walls, or even houses. This may be true as a practical matter, but unfortunately, I am not sure I can think of a single theory of the Fourth Amendment in which that would not be true. It is certainly no less true of the model proposed here than the current doctrine, and any property-based regime afford greater protection to owners of more property. It is the focus on the home that creates this problem. The characteristics of a person’s home affect the degree of privacy it affords, from the homeless to owners of palatial estates. To achieve better equality in privacy, society should create greater economic equality, allowing people to purchase better privacy protection. Perhaps this observation counsels that society should at a minimum provide public places of guaranteed privacy, but that is another thought for another day.

178 Note that these two are different degrees of intrusion as well. The ear to the door is something anyone may do, but the microphone is not and is more intrusive. See Kyllo, 533 U.S. at 35-40 (discussing “through the wall” technology).

179 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.
come out in favor of the government.\textsuperscript{180} The reason the Court would have seen it differently would be the lack of technology, but in the framework proposed here, it is a matter of state action. Undoubtedly technology is responsible for many of today’s changing information flows, but rather than analyze the technology directly, or its general availability, as the \textit{Kyllo} Court did, the cases should analyze a technology’s effect on information flows, just like they should analyze the effect of a new law or police practice.\textsuperscript{181} Whether or not technology is involved, if police act to disrupt an information flow in an unexpected way, that’s the violation. This is discussed at greater length in Part V, but it is mentioned here to point out that the specific technology does not factor into the decision. If the police need the aid of a device or of a dog, then, they are taking an action to change information flows, and ipso facto, the Fourth Amendment is implicated.\textsuperscript{182}

Assuming drug dogs are reliable, then,\textsuperscript{183} the Court’s reasoning that they only detect the presence of something the possession of which is always illegal has merit for the \textit{degree} of suspicion required. Perhaps instead of a warrant, police only need RAPS because the search is necessarily less intrusive. This still avoids the current problem of allowing police to bring drug dogs indiscriminately into every encounter with a car, even among DUI stops or parked cars.\textsuperscript{184} The same is true of thermal

\textsuperscript{180} \textit{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.”)

\textsuperscript{181} See infra Part V.

\textsuperscript{182} The Supreme Court has granted certiorari in \textit{Florida v. Jardines}, which presents the flowing two questions: “1) Whether a dog sniff at the front door of a suspected grow house by a trained narcotics detection dog is a Fourth Amendment search requiring probable cause? 2) Whether the officers' conduct during the investigation of the grow house, including remaining outside the house awaiting a search warrant is, itself, a Fourth Amendment search?” [CITE cert grant]. This case should examine the conflict directly, but I am not confident the Court will see the similarities and reform the jurisprudence, because they have the easier out of recognizing the dogs as a technology unavailable to the population at large.

\textsuperscript{183} They are, however, almost certainly not. See Lisa Lit, Julie B. Schweitzer & Anita M. Oberbauer, \textit{Handler Beliefs Affect Scent Detection Dog Outcomes}, 14 \textit{Animal Cognition} 387 (2011).

\textsuperscript{184} \textit{Caballes}, 543 U.S. at 422 (Ginsburg, J., dissenting). (“Today's decision, in contrast,
imagers – though because they’re more invasive, perhaps a warrant is required. However, 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 takes away the ability to rein in abuse or even debate what the correct level of suspicion or oversight should be.  

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, however. Roving wiretaps serve as one example. Roving wiretaps are wiretaps that have a person as a target rather than a specific phone number. Traditional wiretaps would require a new authorization each time there was a new phone number to monitor, but 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, such as switching phones.  

Roving wiretaps were authorized federally in the Electronic Communications Privacy Act, which updated Title III to include them, after it became clear that criminals were evading traditional wiretaps by changing cell phones.  

The Supreme Court has not weighed in on the constitutionality of roving wiretaps, but all the Circuit courts to consider it have found them constitutional. Each of these cases has said that the particularity requirement for a “place to be searched” was the place in which the suspect was talking. This seems like a twist of logic, but in truth, the concept of “searching” an audio track is inherently divorced from place anyway. Thinking about roving wiretaps in a social context makes them an even easier case. 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. Right now, an application for a roving wiretap has to show that the target has tried to evade traditional wiretaps. A social context-driven theory might instead say that all wiretaps should be roving because it is a person that is the target, not a

---

185 See infra notes 337-342 and accompanying text (discussing the proportionality principle).


188 See, e.g., U.S. v. Bianco, 998 F.2d 1112, 1124 (2d Cir. 1993); U.S. v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996); U.S. v. Wilson, 237 F.3d 827, 831 (7th Cir. 2001).

place, and that is it expected that phone communications will flow to the police, once the warrant is obtained.

IV. PUTTING CONTEXT IN CONTEXT

While a context-focused search doctrine might be new, context has always been present in other areas of the Fourth Amendment.\textsuperscript{190} Every part of the doctrine has scope limitations that restrict a search to its proper context – from warrants\textsuperscript{191} and searches incident to arrest,\textsuperscript{192} to automobile searches\textsuperscript{193} and administrative searches.\textsuperscript{194} In fact, context is written directly into the Fourth Amendment: “. . . and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and \textit{particularly describing the place to be searched, and the persons or things to be seized}.”\textsuperscript{195} 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.\textsuperscript{196} This inherent contextual limitation is the direct consequence of free society’s disdain for general warrants, which drove the Framers to draft the Amendment in the first place.\textsuperscript{197} 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. This Part highlights a few areas of current doctrine that are explicitly context-sensitive, and illustrates that context can be a unifying principle to understand the broader Fourth Amendment.

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.\textsuperscript{198} Courts have

\textsuperscript{190} E.g. Terry v. Ohio, 392 U.S. 1, 19 (1968) (“The scope of [a] search must be ‘strictly tied to and justified by’ the circumstances which rendered its initiation permissible.” (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring))).

\textsuperscript{191} U.S. CONST. amend. IV.

\textsuperscript{192} Chimel v. California, 395 U.S. 752 (1969)

\textsuperscript{193} Arizona v. Gant, 556 U.S. 332 (2009)

\textsuperscript{194} 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”).

\textsuperscript{195} U.S. CONST. amend. IV (emphasis added).

\textsuperscript{196} YALE KAMISAR ET AL., MODERN CRIMINAL PROCEDURE 305-08 (11th ed. 2005).

\textsuperscript{197} Amsterdam, \textit{supra} note 71, at 411.

\textsuperscript{198} 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.”)
gone back and forth arguing about where to draw the balance, but the principle of limited scope is so basic that the arguments are never whether the scope need be limited, but rather how tightly to restrict it. Scope limitations essentially function as partial transmission principles. For example, in the case of warrant exceptions, the principle says that in a particular context, a particular warrant exception is permitted, for a particular, limited purpose beyond which the search must not extend. Unsurprisingly, then, discussions of scope in the various cases follow well 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. However, 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 similar. That is, the argument parallels the normative layer of contextual integrity, recognizing a prima facie violation but arguing it should be the new rule.

Take, for example, the “search incident to arrest” warrant exception. The modern version of the exception, derived from *Chimel v. California*, 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.\(^\text{199}\) According to the Court, danger to the police or possible destruction of evidence justified the exception, thus it must be limited to the physical area in which those are valid concerns – the area of “immediate control.”\(^\text{200}\) The Court specifically observed that it was less reasonable “to search a man's house when he is arrested on his front lawn—or just down the street—than it is when he happens to be in the house at the time of arrest, and then used that to argue that the justifying search must be limited by some principle. Had these rationales come out of contextually analyzed cases, the normative layer would have shown these rationales to be acceptable, as long as they are limited as narrowly as possible, just as the Court said in reality. 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 it only to the areas representing a legitimate danger.\(^\text{201}\) Under contextual analysis, given

\(^{199}\) 395 U.S. 752, 763 (1969). Note that the Court did not define a new exception here, but rather reexamined the doctrine because it did not have a solid normative basis. The decision to narrow the scope 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.

\(^{200}\) *Id.* at 762-63.

the existence of the prior normative result, it is not clear that this extension would even have caused a prima facie violation. The context is the same, as is the rationale permitting the disruption in information flows. Either way, though, the result would be the same.

Eventually 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.\(^{202}\) The end result was a justification for searching the entire car, but the reasoning is what matters. The rationale from Chimel, with its associated scope limitations, was imported in full, rather than starting from a “reduced expectation of privacy” in automobiles.\(^{203}\) 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.\(^{204}\) 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, the Court performed a recalibration similar to Chimel itself.\(^{205}\) Once the arrestee is secured and out of the vehicle, the danger justification disappears, and 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.\(^{206}\) This is just like the suspect being arrested on his front lawn rather than inside the house, as discussed in Chimel.

The particularity and timing requirements for warrants are another area where the scope is limited.\(^{207}\) For a search warrant to be valid, it usually must specify a place and time\(^{208}\) for the search, and the scope cannot exceed what is listed, except what is in plain sight or justified by an exception that otherwise governs warrantless searches. Thus, 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.

\(^{204}\) In Chimel, the Court did address whether it mattered that the arrestee was secured, but presumably that changes the area “within his immediate control.” 395 U.S. at 763.
\(^{206}\) Id.
\(^{207}\) KAMISAR ET AL., supra note 196, at 306-09.
\(^{208}\) This is apparently not a constitutional requirement, but many states limiting warrants to daytime and a short – usually 10-day – execution window. Id. at 308.
The similarity between these scope limitations is their focus on space and time. However, contextual integrity is about social contexts, not spatial, so does this really fit with the theory? Indeed it does. Katz said that the Fourth Amendment governs “people, not places,” and yet a strong focus on the home persists today, with a lesser focus on automobiles. The answer is that a location-based theory of the Fourth Amendment and contextual integrity overlap with respect to these contexts. Society has “overriding respect for the sanctity of the home,” a person’s only place where she can escape the outside world. Therefore, it is not just a place, but also a social context, and it deserves its own protection. The same can be said of the automobile. 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. Thus the 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:

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.’

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

---

211 Gant, 556 U.S. at 345.
213 See Strandburg, supra note 23, at 494 (“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.”)
214 Gant, 556 U.S. at 343 (referring to “circumstances unique to the vehicle context”).
215 Well, that is, unless a person is regularly pulled over for “driving while black,” but searches on that basis are not exactly what we should be basing search doctrine on. See David A. Harris, 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.
doctrines are less spatially tied, and directly limit information flow disruptions in different ways.

B. Stops

Whether a police encounter counts as a “stop,” requiring reasonable suspicion as a “seizure” under the Fourth Amendment, is a question relying on an awareness of social context. \(^{217}\) At the outset, it is clear that if the police use physical force, there is a seizure. \(^{218}\) The more interesting question is when a show of authority by police overrides consent. *California v. Hodari D.* 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. \(^{219}\) It does not require much imagination to see that this is a rule heavily steeped in social context. Shows of authority include brandishing a weapon, \(^{220}\) visibly displaying badges, \(^{221}\) yelling “Stop! Police!” \(^{222}\) – basically those things that would inform a reasonable person that he should submit.

Both the appearance of authority and likelihood of submission vary depending on context. Walking down the street, minding one’s own business would probably require a greater showing to convince a person to stop than if the person was a student in a school or driving a car. In the words of the Court, from a case involving a defendant stopped while seated on a bus with no way to leave: “[T]o 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.” \(^{223}\) The resulting rule is that context is 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. Administrative searches are based on “special


\[^{218}\text{*Hodari D.*, 499 U.S. at 625}\]

\[^{219}\text{Id. at 628.}\]

\[^{220}\text{United States v. Drayton, 536 U.S. 194, 205 (2002).}\]

\[^{221}\text{*Bostick*, 501 U.S. at 446 (Marshall J, dissenting).}\]

\[^{222}\text{*Hodari D.*, 499 U.S. at 626.}\]

\[^{223}\text{*Bostick*, 501 U.S. at 439 (majority opinion).}\]
"needs" that cannot be met by traditional criminal investigation, justified "only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable." 224 Examples include inspections of housing for compliance fire and health code,225 border searches, 226 searches of students in schools 227 and airport security screenings.228 Each of these types of search 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,229 that the formal justification for these searches is context-based illustrates the importance of context to this doctrine.

The framework for administrative searches comes from Camara v. Municipal Court, 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.230 The Court’s definition of reasonableness "balanced the need to search against the invasion which the search entails."231 The Court put forth three factors making up the test: 1) The long judicial and 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."232 This balancing test could have come from contextual integrity directly: The first factor suggests that people would not be surprised by such a search, the second factor goes to the normative layer, and the third explicitly states that the search cannot bleed over into a use – 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

227 T.L.O., 469 U.S. 325.
228 E.g., United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007).
229 See Eve Brensike Primus, Disentangling Administrative Searches, 111 COLUM. L. REV. 254, 255-56 & n.14, n.15 (collecting critiques of the practical results of administrative search cases).
231 Id. at 537.
232 Id.
teachers may “assur[e] discipline and order.” 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,” 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.” 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. Fixed checkpoints can be used for sobriety checks and immigration checks near borders, but those are not good enough reasons to get an administrative warrant in someone’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. Businesses with liquor licenses do not receive as much Fourth Amendment protection, nor do an auto junkyards or sellers of firearms during business hours. Vehicle checkpoints for immigration checks are restricted to those places where motorists will not be taken by surprise— that is, at the border— while sobriety checkpoints are not so restricted. 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. That is, the attribute requested results in different worries about the encounter.

235 Id. at 725.
238 Marshall v. Barlow’s Inc., 436 U.S. 307 (1978). This suggests that perhaps the “chemical market” context is just as salient as the “market” context in Knotts, though “highly regulated businesses” might be the correct context. See discussion of United States v. Knotts, 460 U.S. 276, supra Part II.C.
242 Martinez-Fuerte, 428 U.S. at 559; Almeida-Sanchez v. United States, 413 U.S. 266, 275 (1973) (holding in part that a search based on a roving patrol could not have been a “border search”).
243 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.”)
245 Ortiz, 422 U.S. at 897.
D. Third-Party Exposures by Police

The last section discussed the prohibition on using administrative warrants for ordinary law enforcement purposes. Because the warrant is issued for a specific purpose, the police cannot also use it for criminal investigation. It turns out that the reverse is also true: police may not take a search warrant that is meant for criminal investigation and expose the inside of the home to third parties “not related the objectives of the authorized intrusion.”\footnote{Wilson v. Layne, 526 U.S. 603, 611 (1999).} In \textit{Wilson v. Layne}, the Court ruled unanimously in a § 1983 suit that a media ride-along by \textit{Washington Post} reporters violated the Fourth Amendment.\footnote{\textit{Id.} at 605.} The ruling was not simply that third parties could not attend the police during a search. Rather it was subtler 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.\footnote{\textit{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. The Court had been explicit about this principle earlier as well,\footnote{Maryland v. Garrison, 480 U.S. 79, 87 (1987) (”[T]he purposes justifying a police search strictly limit the permissible extent of the search”).} but this case provides the most concrete example.

\textit{Wilson} has not been tested again in the Supreme Court, but the Second Circuit has had two opportunities to expound on the doctrine. In \textit{Lauro v. Charles}, the court ruled that a “perp walk,” the sole aim of which “was to seize and broadcast images” of the arrestee and thus “needlessly infringe[e] his privacy” was unconstitutional.\footnote{219 F.3d 202, 213 (2d. Cir. 2000).} The court read \textit{Wilson} to
stand for two principles:

One, the reasonableness requirement of the Fourth Amendment applies not only to prevent searches and seizures that would be unreasonable if conducted at all, but also to ensure reasonableness in the manner and scope of searches and seizures that are carried out. Two, the reasonableness of the police's actions in conducting a search or seizure must be judged, in part, through an assessment of the degree to which those actions further the legitimate law enforcement purposes behind the search or seizure.²⁵¹

Similarly to the Supreme Court in Wilson, the Second Circuit here made sure to point out that it was not prohibiting incidental photography during an arrest,²⁵² but only “conduct that was unrelated to the object of the arrest, that had no legitimate law enforcement justification, and that invaded Lauro's privacy to no purpose.”²⁵³ Again, those things that narrowly aid the police are permitted in an arrest situation, which is strongly in the law enforcement context.

In Caldarola v. Westchester, the Second Circuit had the opportunity to consider the unstaged perp walk.²⁵⁴ Lauro had explicitly reserved the question, and the Caldarola court relied on Lauro’s rationale, eventually stating that this perp walk served law enforcement purposes.²⁵⁵ The Second Circuit then had to contend with Wilson because the law enforcement purpose it relied on, “educating the public about law enforcement efforts,”²⁵⁶ was explicitly rejected in Wilson as an unrelated purpose.²⁵⁷ The Court in distinguished these facts by explaining that the reporter did not invade the plaintiff’s home, but rather pulled him in front of reporters when he was already in public.²⁵⁸ In light of Lauro and Wilson’s focus on the context, this distinction is rather unconvincing. Wilson said educating the public was not a purpose for the particular interaction with the police, but

²⁵¹ Id. at 211 (quotation omitted).
²⁵² Id. at 213. (“It is important, however, to understand the limitations of our holding. First, we do not hold that all, or even most, perp walks are violations of the Fourth Amendment. Thus, we are not talking about cases in which there is a legitimate law enforcement justification for transporting a suspect. Accordingly, we do not address the case—seemingly much more common than the kind of staged perp walk that occurred here—where a suspect is photographed in the normal course of being moved from one place to another by the police. Nor do we reach the question of whether, in those circumstances, it would be proper for the police to notify the media ahead of time that a suspect is to be transported.”)
²⁵³ Id. at 213.
²⁵⁴ 343 F.3d 570, 573 (2d. Cir. 2003).
²⁵⁵ Id. at 572.
²⁵⁶ Id.
²⁵⁸ Caldarola, 343 F.3d at 577.
rather too general a police interest. That the plaintiff was outside in *Caldarola* did not change that. The case reads as a weak attempt to thread the needle, further demonstrating that social context drives this doctrine.

V. TECHNOLOGY AND THE FUTURE OF SEARCH LITIGATION

New technology is at the heart of many contemporary disruptions of information flows. Accordingly, an understanding of how to treat technology is central to an approach to future Fourth Amendment search doctrine. The most important thing to recognize about technology is that it is in a sense not special. Technology can disrupt information flows in exactly the same ways that a new law or new policy can, and the privacy backlashes in the news are usually the result of the coupling of new technology and new policies. For example, Facebook as a technology has changed information flows drastically, allowing people to share widely and preserving information indefinitely, but when analyzing the emerging trend of employers asking for Facebook passwords, the technology is just one factor alongside the policy itself.\(^{259}\) Similarly, GPS has disrupted information flows regarding location, but the FBI’s decisions about how to deploy GPS trackers are just as important to determining whether there is a violation of informational norms. Technology is intimately intertwined with the social context in which it is created or used. Accordingly, just like any other information flow disruption, it 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. The discussion of technology in these cases focuses on the technology qua technology, rather than analyzing its effects. In order for law to respond to changing technology and be coherent over time, it must be technology-independent. The cases instead contain technology-dependent idiosyncrasies in rationale and result. In *Knotts*, the Court suggested that the beeper only allowed police to observe what they otherwise could by the naked eye, and thus that the technology was unimportant to the decision.\(^{260}\) This conclusion could be supported by a contextual analysis too, saying that the information flows due to the technology didn’t change much from a standard situation of police following a subject, thus the rules of a physical following situation would apply.\(^{261}\) The difference between approaches is in


\(^{261}\) See Part III-B-3, *supra*. We are not saying that this is the proper conclusion, only
this case minimal because the reason for the dismissal of the technology is essentially its low impact on information flows.\textsuperscript{262}  

\textit{Kyllo} similarly gets it right, at least with respect to the information flows. 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.\textsuperscript{263} 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, to take deliberate action – to “search” – to find out that marijuana is being grown in the house.\textsuperscript{264} The Court then went on to say that once such a technology is in general use by the public, there is no expectation of privacy.\textsuperscript{265} If the Court were analyzing information flows rather than technology, this result would have been different. If the technology were publicly available and the general, socially acceptable public use were the same as the police use, then the use would be acceptable because it did not contravene entrenched informational norms.\textsuperscript{266} However, reasoning about the availability of the technology without further examination into the resulting typical, appropriate (by this hypothetical society’s definition) information flows gets it wrong. What matters is not the technology, but the informational norms, even if the availability of technology itself has coincided with 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. 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.”\textsuperscript{267}  

---

\footnotesize{\textsuperscript{262} Id. (“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.”)}

\footnotesize{\textsuperscript{263} Kyllo v. United States, 533 U.S. 27, 34 (2001).}

\footnotesize{\textsuperscript{264} See id. at 35 & n.2}

\footnotesize{\textsuperscript{265} Id. at 34.}

\footnotesize{\textsuperscript{266} 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.}

\footnotesize{\textsuperscript{267} United States v. Jones, 132 S.Ct. 945, 958 (Alito, J., concurring.)}
Sotomayor likewise stated of her analysis:

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.\(^{268}\)

This treatment of technology is fundamentally correct. As commentators were quick to point out, though, the concurrences lacked a test or framework\(^{269}\) for determining exactly what qualifies as “longer term GPS monitoring” subject to the Fourth Amendment.\(^{270}\) This question can be resolved by balancing the interests that emerge from the analysis of the changing information flows in the normative layer of a contextual Fourth Amendment. Most likely, this means the specific solution will be fleshed out over several cases, in common law fashion. A contextual Fourth Amendment provides structure in which to make the decision, though it cannot make the normative valuation alone. Because the Court has already addressed GPS, this section examines a few other technologies increasingly commonly used by law enforcement – cell phone location data,\(^{271}\) visual surveillance and recording, such as automatic license plate recognition (ALPR),\(^{272}\) surveillance cameras\(^{273}\) and drones,\(^{274}\) and social networks\(^{275}\) – and discusses how a court might think about them.

### A. Cell Phone Location Data

Cell phone location data offers an even more complete picture of a

---

\(^{268}\) Id. at 956 (Sotomayor, J., concurring).

\(^{269}\) Goldstein, supra note 4.

\(^{270}\) Jones at 964 (Alito, J., concurring).


person’s whereabouts than GPS. The GPS tracker in Jones had to be installed in a person’s car, but phones automatically track location for the purposes of providing service, just by virtue of being turned on. Additionally, people carry their phones with them at all times of day, even routinely sleeping with their phones on their nightstands.\textsuperscript{276} Cell phone carriers then keep this data for a long time, usually a year or more.\textsuperscript{277}

Police routinely use cell-phone location data to track people.\textsuperscript{278} The typical information flow is as follows: As a prerequisite, cell phone location data is collected by the carriers as mandated both by pure functionality and by law for emergency services.\textsuperscript{279} The service providers then store the data. This storage may or may not be justified,\textsuperscript{280} but regardless, the information flow of interest here is the further one in which the police (receiver) obtain the data from the carrier (sender) about the customer (subject). The police often obtain everything that the phone company stores, such as text messages and phone numbers dialed, but this discussion is about location data specifically. The trick here is to identify the transmission principle.

\begin{footnotesize}
\footnotesize


\textsuperscript{278} The \textit{New York Times} recently ran a front page story about local police departments’ use of this practice, which might be more surprising to people than the thought that the FBI is doing the same. Lichtblau, supra note 271. The practice is so common that in Antoine Jones’s retrial (necessitated by the Supreme Court’s ruling 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, \textit{After Car-Tracking Smackdown, Feds Turn to Warrantless Phone Tracking}, \textsc{Threat Level} (Mar. 31, 2012), available at, 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 cell phone technology or equipment used to locate the targeted subject.” Lichtblau, supra. The training manual also advised the tracking be kept out of police reports. \textit{Id}. The expected outrage is, as always, good evidence that the practice would violate informational norms.

\textsuperscript{279} Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414 (1994).

\textsuperscript{280} 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 educated about the data storage would have would not allow this, and it’s hard to talk about a norm existing when a practice 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.
\end{footnotesize}
Given the speed with which norms in this area are changing due to the advancement of technology, however, identifying the specific transmission principle is nearly impossible. An easier task is to define what it prohibits.\textsuperscript{281} To the extent the data collection is justified, it is for the limited purpose of phone functionality, 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 don’t even recognize that the phone company collects this data would find its transmission to the police appropriate without a warrant. Thus, police acquisition of this information without a warrant or warrant exception such as exigency (perhaps in the true ticking time bomb scenario) would violate the Fourth Amendment. A rule by which the police could obtain this data simply by virtue of its existence would mirror the rule in the banking context, essentially conditioning all cell phone use on a waiver of Fourth Amendment rights.\textsuperscript{282} Such a rule would be even more troubling than the banking context because a phone company knows a lot more about a person and his whereabouts than a bank does.

Police use of cell phone location data is actually making its way through the courts now, and some of the briefs are showing how to use contextual arguments in current litigation.\textsuperscript{283} In \textit{State v. Earls}, a case pending in the Supreme Court of New Jersey, the police contacted the defendant’s cell phone carrier three times between 8PM and 11PM one night in order to find him to arrest him.\textsuperscript{284} The police found the defendant in a motel room that contained stolen goods.\textsuperscript{285} When the defendant tried to have the stolen goods suppressed, the trial court denied the motion and the Appellate Division upheld the decision, based on \textit{Knotts} and “no privacy on public roads.”\textsuperscript{286} The Electronic Privacy Information Center (EPIC) filed an

\textsuperscript{281} Throughout this section, I attempt to frame the transmission principles as uncontroversially as possible. For more specific understandings of the norms

\textsuperscript{282} See text accompanying supra note 118. Just to be clear, I am not suggesting that cell phone use is a fundamental right, just like access to the banking system is not. Rather, I am saying that if something is not a fundamental right, that does not imply its use is entirely voluntary, either, and that normatively, it is insane to condition use of all cell phones on a waiver of Fourth Amendment rights.

\textsuperscript{283} Much of this Article has argued that the relevant precedent is wrong for one reason or another. Given that, it would be possible to imagine that contextual arguments would not be useful in current litigation, but these examples from the briefs show that to be incorrect. As the beginning of this section illustrates, the actual approach of much of the technology-related precedent is not that far off, even if the end results are questionable. So at least for new technologies, a contextual and technology-independent approach is fairly consistent with the relevant precedent.


\textsuperscript{285} \textit{Id.} at 118.

\textsuperscript{286} \textit{Id.} at 124; see also supra Part III-C.
amicus brief in the pending case, which treats technology exactly correctly as an agent of changing information flows, rather than the focus of the case itself.\textsuperscript{287} The brief notes that cell phone location is a proxy for personal location\textsuperscript{288} because people carry around cell phones and they are “necessary for work, school, and everyday social and political life and kept on their person at all times.”\textsuperscript{289} This situates the cell phone in its social context. Following that is an observation that at least in urban areas, cell site data is more effective at pinpointing people than GPS.\textsuperscript{290} The brief also stresses the amount of data that can be collected about a person and how revealing that is, quoting the “mosaic theory” statement from \textit{United States v. Maynard}:

\begin{quote}
A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.\textsuperscript{291}
\end{quote}

In addition to New Jersey, the Fifth Circuit is hearing \textit{In re: The Application of the United States Of America for Historical Cell Site Data}, an appeal from a district judge’s affirmation of a magistrate’s holding that the Fourth Amendment precludes the use of cell site data without a warrant.\textsuperscript{292} The decision was based in part on Third and Sixth Circuit precedents saying that third party doctrine does not apply, though the Third Circuit precedent remanded to the district court for the constitutional question.\textsuperscript{293} and the Sixth Circuit held that \textit{Knotts} controlled and the Fourth Amendment was not implicated.\textsuperscript{294} Notably, the lower courts in this case (that required a warrant) acted before \textit{Jones} was decided, based on the invasiveness of long-term cell site tracking. Just like in New Jersey, now that \textit{Jones} has called the absolutism of \textit{Knotts}’ “no privacy in public” reasoning into question, the Fifth Circuit will have to determine how to proceed. In this case, EPIC once again filed a context-based brief, one subheading of which reads: “Service Providers Configure Telephone

\footnotesize
\begin{itemize}
\item \textsuperscript{288} \textit{Id.} at 12-13.
\item \textsuperscript{289} \textit{Id.} at 5.
\item \textsuperscript{290} \textit{Id.} at 5-9.
\item \textsuperscript{291} \textit{Id.} at 12 (quoting \textit{United States v. Maynard}, 615 F.3d 544, 562 (D.C. Cir. 2010) aff’d in part sub nom. \textit{United States v. Jones}, 132 S. Ct. 945 (U.S. 2012)).
\item \textsuperscript{292} \textit{747 F.}Supp.2d 827 (S.D. Tex. 2010).
\item \textsuperscript{293} \textit{Id.} at 830.
\item \textsuperscript{294} \textit{Id.} at 843 n.90 (citing \textit{United States v. Forest}, 355 F.3d 942, 950-51 (6th Cir. 2004)).
\end{itemize}
Systems To Automatically Generate Cell-Site Data In Order to Comply With Federal Wiretap Laws, a Purpose Unrelated to the Delivery of Cellphone Service." The unrelated purpose is central in a contextual account. The next section argues that people do expect that they can shield their location data and often make efforts to do so, and like in the Earls brief, makes an explicit connection between reasonableness and respect for context.

B. Pervasive Visual Surveillance and Recording

Several of the growing technologies have similar effects on information flows. ALPR systems read and record license plates of cars that pass their cameras. Ubiquitous surveillance cameras film every passerby, capturing and storing full streams of their entire visual fields, and drones do the same while flying around, only at greater capacity and resolution. Combined with advancing facial recognition technology, the visual surveillance from stationary and drone-mounted cameras has a potential for automation and searchability, while the ALPR system naturally contains those attributes.

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

---

296 Id. at 24-26.
299 Id.
300 Id.
301 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?’)
York, there is an even higher density of surveillance cameras. In 2005, the organization found 4468 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 5 square miles in Manhattan. 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. One drone currently in use in Afghanistan has the ability to scan the area of a small town. According to a general, “analysts will no longer have to guess where to point the camera. . . . The drone will be looking at a whole city, so there will be no way for the adversary to know what we’re looking at, and we can see everything.” The domestic use of drones has increased in large part due to their success abroad, 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. The drones’ capability to surveil an entire population in plain sight without possibility of detection is only held back by their relative expense and later adoption.

In future 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 that can be done writ large. This is actually pretty similar to Justice Alito’s suggestion in Jones, stating that long-term surveillance is the problem, with no more specificity. The debate has already begun to move toward the merits of “mosaic theory,” which states that the composite picture is greater than the sum of its parts and should

---


303 Manhattan’s total area is 23.7 square miles, http://www.nycgo.com/articles/nyc-statistics-page. 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.


307 United States v. Jones, 132 S.Ct. 945, 958 (Alito, J., concurring.)
thus be limited.  

Contextual analysis of these technologies requires an examination of each of their information flows, specific to each type of information gleaned. Except for the information in ALPR, the attributes in these flows are a whole host of different types of information, from physical whereabouts, to clothing choices, to a person’s associations – anything that could come from tracking a face 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, as mosaic theory would.

For the sake of brevity, the three technologies can be analyzed together because their information flow disruptions are similar. All three technologies alter information flows in three ways: 1) by making 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 complicate the transmission principles, but it seems likely that people would expect to have a measure of control over most of this information, though with respect to some information, norms might be changing.

Step 1, 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 in some sense could 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. One of the unanalyzed problems with Knotts was that it extended the ability of police to follow absent detection. These technologies, at least in Step 1, are just extreme expansions of the Knotts beeper.

Step 2, the recording, is problematic in the same way that recording any of the emanations or conversations is. Systematic recording changes the flow of “public” observations from what people expect from their knowledge of the limits of human perception and recall. Additionally, by recording now and analyzing only later, the devices can capture information

---

309 For ALPR, mosaic theory and the contextual analysis would be similar, as location is really the only information type being transferred.
310 Nissenbaum, supra note 17, at 145, 192.
311 See supra Part III-B and III-D.
faster than a human, and thus capture more information. It is impossible to imagine, for instance, the police officer capable of writing down 1800 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.\textsuperscript{312}

Step 3 is also invasive, turning what would otherwise be an unmanageable pile of individual images and numbers into searchable databases. As a matter of technological possibility, searchability is much more prevalent in ALPR than the photo databases. Capturing and digitizing license plate numbers is a much easier technological problem than facial recognition. Facial recognition is much more challenging because of the high degree of variability in faces and background conditions.\textsuperscript{313} However, with the aid of other contextual information, such as residential location and social networks of associates, off-the-shelf facial recognition software may allow the police to accomplish the task.\textsuperscript{314} An additional difficulty for facial recognition has historically been that faces were not available in a database with which to compare, unlike license plates. Thus, facial recognition has so far been used to compare faces only to criminal databases.\textsuperscript{315} Recent research has demonstrated, however, that Facebook is solving both the lack of facial picture databases and the contextual problem of identifying them.\textsuperscript{316} Eventually, it is easy to imagine that facial identification could

\textsuperscript{312} The ACLU of New Jersey’s brief in \textit{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.


\textsuperscript{316} Id.
simply become a matter of access to Facebook’s database and computing power. In all these cases, the ability to search after the fact is the thing that makes indiscriminate collection of data useful in the first place, rather than requiring resource decisions based on individualized suspicion. There is really no way to speak about an analogue in people’s expectations for this step, because searchability of a database is never important until there is more data than current privacy expectations would likely permit.

These technologies surely represent departures from the typical in-person police surveillance and investigation techniques presented in *Knotts* and in society’s broader understanding of police work. The normative layer of analysis requires separation of the flows as well. Society probably views it as more of a breach to search the data for a person’s religion than for whether he has a dog. In the former case, the police’s knowledge of a person’s religion or use of that knowledge is potentially harmful to the context of religious worship generally, but the knowledge of a person having a pet probably does not hurt the context of home life. The difficulty with these technologies is that they cast so broad a surveillance net that they intersect every imaginable social context, but the discussion remains manageable when grounded in those contexts.

**C. Online Social Networks**

Social media like Facebook and Twitter are almost certainly a context unto themselves. There are developing norms about what to post where, and how much to share. These norms are being shaped by the available technologies, but when the technologies change and a backlash is triggered, it becomes clear that the technology is not simply driving the norms. Describing the expected information flows on Facebook, however, is incredibly difficult. If a user limits a post to her own friends, the user expects her friends to be able to see it, and further, she is relying on informational norms in the “friendship” context to curb future dissemination. Thus depending on the specific information she shares, her friends should know whether it is sensitive and to what level. 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. If a user instead allows “friends of friends” to

---


see a post, it is in some sense more public, but less than a fully public post; it does not, for example, come up in search results. There is less of an expectation that a “friends of friends” post will not make its way somewhere undesired, because a user has limited, if any, control over who exists at the second level of the network.\textsuperscript{319}

Importantly, however, evidence suggests that many users of Facebook simply do not understand how their privacy settings work in practice,\textsuperscript{320} or that they even exist at all.\textsuperscript{321} The lack of knowledge about how information is \textit{actually} flowing makes it very difficult to discern the informational norms for online networks, even as much as they have developed. In part, they are similar to the familiar contexts in society, especially where people have the option of disaggregating groups into “circles”\textsuperscript{322} or “lists”\textsuperscript{323} of acquaintances, colleagues, family, or friends. But

\textsuperscript{319} Lior Strahilevitz has argued for more generally for a “social network” theory of privacy, which would suggest a reasonable expectation at the “friend of friend” level, but not beyond. Strahilevitz, \textit{supra} note 20, at 967-68 (“An illustration will be helpful: extramarital affairs are fascinating events. That said, no self-respecting person would go to a cocktail party and tell a private story about a friend of a friend of a friend who is having an adulterous affair with someone unknown to the speaker and listener. It is only if the speaker or listener knows who the adulterers are, or if the details of the affair are particularly sordid, humorous, or memorable, that the information is likely to get disseminated further through the social network.’ And by the time the information makes it through this chain, it seems likely that the participants’ names would have dropped out of the story.” Thus, when dealing with events described via word of mouth, someone should have a reasonable expectation of privacy beyond two links in a social network.”) However, his analysis is based on word-of-mouth communications, and (as he acknowledged with respect to email and blogging) being online with easy broadcasting capabilities changes things. \textit{Id.} at 968. Adapting his cocktail party example,\textsuperscript{319} it is just as unlikely that a person will tell all 300 of his online “friends” the lurid details of his affair as it is that he will share the details of a “friend of a friend of a friend.” Therefore it is clear that the magnitude of these online broadcasts is definitely wider than word of mouth dissemination, and “friend of a friend” is more public on Facebook than in person.

\textsuperscript{320} Bernhard Debatin, et al., \textit{Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences}, 15 J. COMPUTER-MEDIATED COMM. 83, 94 ([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.”)

\textsuperscript{321} See \textit{supra} note 325.


\textsuperscript{323} How do I use lists to organize my friends?, 
the ability to communicate with all of your friends at the same time is new, and few people do disaggregate lists, leading to “collapse of contexts.”

Twitter posts have a slightly different dynamic. Either they are protected or completely public. If they are public, the posts can be seen by going to twitter’s website without even logging in, and the information should be treated as public. If they are protected, then they function similarly to the “friend” level of posts on Facebook.

Unsurprisingly, online social networks are another wealth of information for police. At the very least, police can easily scan any information that is unprotected by any privacy settings. That includes any public postings, but also most friend/follower lists, because Facebook and Twitter have made them public (Facebook by default and Twitter as the only option). Legally, this information is governed by the plain view doctrine, and thus does not implicate the Fourth Amendment. More interestingly and provocatively, police have also set up fake social media accounts in attempts to track some criminal suspects – a practice sure to gain currency in the future. One study showed over 40% of users willing

https://www.facebook.com/help/?faq=200538509990389

324 Marwick & boyd, supra note 317.

325 Defaults are incredibly important, as relatively few people change them as a general matter. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 35, 83-87 (2008). However, it does appear that all the publicity about privacy has gotten the number of users that change their settings to more than half, Emil Protalinski, Facebook CTO: Most People Have Modified Their Privacy Settings, ZDNET (Oct. 20, 2011), https://www.zdnet.com/blog/facebook/facebook-cto-most-people-have-modified-their-privacy-settings/4767, though with constant changes, it has been very difficult for even those people to keep up. Rob Waugh, Half of Facebook Users 'Can't Keep Up' With Site's Snooping Policies as Privacy Rules Change EIGHT Times in Two Years, DAILY MAIL (Nov. 3, 2011), http://www.dailymail.co.uk/sciencetech/article-2057000/Half-Facebook-users-sites-snooping-policies-site-changes-privacy-rules-EIGHT-times-years.html.

Facebook also does not make it obvious how to hide a friends list. In its current settings iteration, the option to hide the friends list is not even located in “Privacy Settings,” but rather, separately, within your friends list, under Edit > “Who can see your full friend list on your timeline?” There is no option to hide people’s mutual friends.


327 Though under this theory, the act of searching for this information online is legally a “search.” See supra Part II-B.

to add strangers as friends on Facebook, \(^{329}\) and given most users do not understand the privacy settings, \(^{330}\) information may be more public than they desire. \(^{331}\) Even assuming a user does understand the settings, if the user has them set so that friends of friends can see her posts or friend list, it is the user’s *friends’* willingness to add the undercover police officer that jeopardizes the user’s privacy. Moreover, if the police officer gets to be friends with several people in the targeted user’s network, the user is going to be more willing to trust the unknown person who is requesting a connection. \(^{332}\) thinking perhaps he met him at a party and forgot afterward, or at the least, that the stranger is not a threat.

Without knowing the rules of this particular social context, a contextual analysis is difficult. The “friendship” context is likely the closest model, and thus the analysis of the pretend friend cases is probably the most similar to police plants on Facebook. \(^{333}\) However, while a user that adds the police officer himself might be said to assume the risk (in the mold of the pretend friend cases), the idea that a police infiltrator who can see the target’s “friend of a friend” posts is entitled to the same benefit is much harder to justify without calling the posts simply “public.” As discussed earlier, however, some sharing is incredibly important, be it with doctors, banks, or as the basis of social relationships. To merely suggest that a post to Facebook is a public post repeats the core misunderstanding that some social sharing is essential to society and should normatively be encouraged.

Professor Strandburg has proposed the web should be thought of as the “home” context, as it is now where we store files and interact with friends. \(^{334}\) Professor Strandburg suggests that “if the ‘occupant’ of the site controls access, and does not make it accessible to the public at large, requiring that law enforcement officials obtain a warrant in order to search

---


\(^{333}\) See supra Part III-B.

\(^{334}\) See Strandburg, supra note 23, at 144 (“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.”)
the activity records of the site seems reasonable.”

Her argument works very well for cloud storage, as a file cabinet has always been protected, but the home is a social context because of its special place in society, and online social networks do not have that same status, meaning the “friendship” context is probably the best model for now.

CONCLUSION

This Article has proposed that we reinterpret Fourth Amendment search doctrine to consider context as a central tenet. If one believes both that contextual integrity does a good job of describing how people in liberal societies actually experience privacy in all its complexity, 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 approach would also unify Fourth Amendment theory behind the concept of context, which already exists by other names throughout the doctrine, such as prohibitions on whom police can bring into a home and scope limitations on searches and warrants.

However, the approach in this Article 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 are implemented all at once, a whole slew of police actions will suddenly become “searches” subject to the Fourth Amendment. While many such searches would be considered reasonable under this approach and thus 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.

Additionally, the Article has left open many normative questions – deciding what searches are or are not reasonable. Contextual integrity is not equipped to make that determination; it can only provide guidelines to frame the normative debate and make sure that at least the inquiries are balancing the correct values, regardless of the result of that balancing. Because of this limitation, this approach implicitly relies on the “wisdom of the common law” to sort out these questions.

Despite the potential for unsettled doctrine, however, the important

335 Id. at 147.

336 This Article is in fact agnostic as to the outcome of those normative debates; if Mark Zuckerberg 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), http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html.
question is not if unsettling the doctrine is unpleasant, but rather, 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 current settled doctrine is so out of step with societal expectations that the dangers of unsettling it do not measure up. The Article already discussed the internal inconsistencies of current doctrine, but its practical effects are dangerous. If third party doctrine is taken seriously, any documents stored online, the contents of any email on a cloud server like email, the content of any text message – basically any digital communication – is outside the purview of the Fourth Amendment, despite more and more of lives actually being lived online.337 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.338 Coupled with the recent decision by the Supreme Court that the good faith exception applies to the exclusionary rule,339 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.

This approach also implicitly relies on a proportionality principle for reasonableness of search, which might well be an administrative nightmare.340 While a substitute approach could also work, to the extent the Article implicitly relies on proportionality, a defense is required. In practice, because clarity in search is indeed important (or at least as much clarity as it is even possible to achieve341), 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 it is overly limited. As Chris 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 essential to

337 Strandburg, supra note 23, at 103.
340 See supra note 71.
341 Slobogin, supra note 71, at 71
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. 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,” “substantial chance,” or “reasonable ground for belief of guilt,” the end result of which is that each standard can be applied to any set of facts, with no clarity at all. The only reason this lack of clarity is permitted now is that it results in extreme deference to police, so they can’t very well complain about the lack of clarity. So while case-by-case proportionality is indeed unworkable, so is the other “bright-line” based extreme of one or two levels of suspicion, and some middle ground is more desirable. Additionally, it is not easy to determine which is “more” or “less” invasive between different types of privacy breaches, and a more discrete spectrum will alleviate that worry as well. Such a discrete spectrum is likely to result from a common law process having learned the lessons of the past.

The concurring justices in Jones seemed to be searching for a new framework to describe their intuition that long-term surveillance was a search, even though it only captured what was seemingly available to the public eye. The executive branch, meanwhile, has begun to accept that context is central to how society experiences privacy. Both President Obama’s Privacy Bill of Rights and the Federal Trade Commission’s recent report on consumer privacy heavily rely on Professor Nissenbaum’s theory in making their privacy recommendations. The

342 Id. at 70-71.
343 A proportionality principle also fits nicely with the original meaning of the Fourth Amendment as described by Akhil 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 Amar, supra note 34, at 778. A proportionality principle also focuses on reasonableness as completely separate 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 qualified immunity doctrine is pulled back some.
345 Id. at 243 n.13. It is pretty remarkable that two different definitions of probable cause actually exist in the same case.
347 [See Erica Goldberg’s new piece]
348 THE WHITE HOUSE, supra note 30, at 15-18.
349 FEDERAL TRADE COMM’N, supra note 31.
350 Alexis Madrigal, The Philosopher Whose Fingerprints Are All Over the FTC’s New
judicial branch can take their cue from the executive. While other frameworks can explain the difference between GPS and a beeper, contextual integrity does the best job of ensuring that the Fourth Amendment has a grounded, and thus reasonable, expectation of privacy.

---