

The Emerging Principles of Fourth Amendment Privacy

Matthew Tokson*

ABSTRACT

The Fourth Amendment applies when the government violates a citizen’s “reasonable expectation of privacy.” But the Supreme Court has never explained what makes an expectation of privacy reasonable, and scholars regularly complain that this standard is incomprehensible and unworkable.

Yet the reasonable expectation of privacy standard may be more coherent than is currently recognized. The Supreme Court has decided more than 40 reasonable expectation of privacy cases since the standard was developed. This Article is the first to analyze all of these decisions. It draws out three consistent principles that drive the Court’s assessments of Fourth Amendment privacy: the intimacy of the place or thing targeted; the amount of information sought; and the cost of the investigation.

The Article traces these principles through the Court’s Fourth Amendment jurisprudence, offering an explanatory account of a body of law often thought to be inexplicable. And it brings them forward, generating predictions for future cases involving novel surveillance technologies.

The Article makes several contributions to the Fourth Amendment literature. It develops a unified model of Fourth Amendment privacy, one that operates consistently across a variety of surveillance contexts. It details the Supreme Court’s growing acknowledgment of the principles of intimacy, amount, and cost. It makes the case for more overt recognition of these principles, which would have substantial benefits for Fourth Amendment jurisprudence and scholarship. And it offers a clear, comprehensible answer to the question of what violates a reasonable expectation of privacy.

TABLE OF CONTENTS

INTRODUCTION	2
I. THE MYSTERY OF THE FOURTH AMENDMENT’S SCOPE	6
A. <i>The Supreme Court and the Katz Test</i>	6
B. <i>The Search for Reasonable Expectations of Privacy</i>	8

* Associate Professor, University of Utah S.J. Quinney College of Law. Thanks to Shima Baughman, Paul Cassell, Cathy Hwang, Orin Kerr, Ronnell Andersen Jones, Amelia Rinehart, Cliff Rosky, Laurent Sacharoff, Jeff Schwartz, and Tammi Walker, and all participants in the Privacy Law Scholars Conference and the Rocky Mountain Junior Scholars Workshop. This research was made possible, in part, through generous support from the Albert and Elaine Borchard Fund for Faculty Excellence. Special thanks to Christian Clark, Emily Nuwan, Connor Plant, Sydney Sell, and Darren Struble for their excellent assistance.

II. THE PRINCIPLES OF FOURTH AMENDMENT PRIVACY ...	13
A. <i>Intimacy</i>	15
B. <i>Amount</i>	18
C. <i>Cost</i>	22
D. <i>A Unified Model of Fourth Amendment Privacy</i>	27
III. EXPLAINING REASONABLE EXPECTATIONS OF PRIVACY	30
A. <i>Reasonable Expectations of Privacy at the Supreme Court</i>	31
1. <i>Standard Cases</i>	34
2. <i>Outliers</i>	38
B. <i>Weighting the Principles and Resolving Close Cases</i>	41
IV. ASSESSING THE PRINCIPLES-BASED APPROACH	43
A. <i>Advantages</i>	44
B. <i>Drawbacks</i>	45
C. <i>The Case for Greater Recognition of the Principles</i>	48
D. <i>Resolving Future Cases</i>	50
1. <i>Drones</i>	51
2. <i>Smart Homes and Devices</i>	53
3. <i>Facial Recognition</i>	55
CONCLUSION	57
APPENDIX	59

INTRODUCTION

The Fourth Amendment regulates government surveillance and prevents arbitrary privacy intrusions. But it only does so in certain contexts. The Supreme Court has held that the Fourth Amendment applies when the government violates an individual's "reasonable expectation of privacy."¹ Yet even as the Court has resolved numerous cases under this standard, it has never explained what makes an expectation of privacy "reasonable."² The Court has refused to commit

1 *E.g.*, *Oliver v. United States*, 466 U.S. 170, 178 (1984). The Supreme Court has recently adopted a separate test that finds a Fourth Amendment search when a government official physically intrudes on property for the purpose of gathering information. *See Florida v. Jardines*, 569 U.S. 1, 7–10 (2013); *United States v. Jones*, 565 U.S. 400, 404–06 (2012). This has, thus far, added little to the *Katz* test, and the Supreme Court cases where it has been employed would likely have reached the same outcome under *Katz*. *See Jardines*, 569 U.S. at 12–16 (Kagan, J., concurring); *Jones*, 565 U.S. at 418–31 (Alito, J., concurring).

2 Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007).

to any stable set of principles that might determine the scope of the Fourth Amendment.³

Indeed, the Court often appears to rely on a rationale in some cases only to expressly reject it in others. The Court has ruled that the likelihood of detection both is⁴ and is not⁵ a determinant of the Fourth Amendment's scope. Its cases establish that property law is either important⁶ or irrelevant⁷ to people's reasonable expectations of privacy. And the exposure of personal information to third parties alternately eliminates⁸ or does not affect⁹ the Fourth Amendment's protections.

The ambiguity of the reasonable expectation of privacy test has troubled courts and scholars for decades.¹⁰ Many have criticized the Court's Fourth Amendment jurisprudence as illogical, erratic, and confusing, among other problems.¹¹ Yet the reasonable expectation of privacy test may be more comprehensible than is currently recognized.

The Supreme Court has now applied the test in over 40 cases since 1967.¹² From this substantial set of cases, consistent principles have begun to emerge.¹³ The Court has increasingly acknowledged the importance of these principles, especially in its recent cases involving

³ *Id.*; see *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (plurality opinion) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.").

⁴ See *Bond v. United States*, 529 U.S. 334, 338–39 (2000); *Minnesota v. Olson*, 495 U.S. 91, 96–99 (1990).

⁵ See *Illinois v. Caballes*, 543 U.S. 405, 408–09 (2005); *United States v. Jacobsen*, 466 U.S. 109, 118–22 (1984).

⁶ See *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978); *United States v. Miller*, 425 U.S. 435, 440 (1976).

⁷ See *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018); *Oliver v. United States*, 466 U.S. 170, 183–84 (1984).

⁸ See *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *Miller*, 425 U.S. at 442–43.

⁹ See *Carpenter*, 138 S. Ct. at 2223; *Ferguson v. City of Charleston*, 532 U.S. 67, 84–85 (2001).

¹⁰ See, e.g., Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010); Scott E. Sundby, "Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?, 94 COLUM. L. REV. 1751, 1771 (1994).

¹¹ E.g., Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 121 (2002); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1325–26 (2012); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 103 (2008).

¹² The Court has issued 50 rulings on Fourth Amendment searches under the "reasonable expectation of privacy" test across 41 cases, several of which involve multiple rulings on several alleged searches. See *infra* app. tbl.1.

¹³ See *infra* Parts II–III.

complex surveillance technologies like GPS and cell phone tracking.¹⁴ Those cases have compelled the Justices to be clearer about their fundamental concerns regarding police surveillance—concerns that transcend concepts like property rights or third-party disclosure.¹⁵ Meanwhile, scholars have analyzed related aspects of privacy in their critiques of Fourth Amendment caselaw, and their work can provide a theoretical basis for a more coherent approach to the Fourth Amendment's scope.¹⁶

This Article draws on all of these sources and identifies three emerging principles that appear to drive the Court's intuitions in Fourth Amendment search cases: the intimacy of the place or thing targeted; the amount of information sought; and the cost of the investigation. By assessing these factors and their complex interactions, observers can better understand how the Court draws the boundaries of the Fourth Amendment.

How do these principles drive Fourth Amendment case outcomes? The Court assesses them explicitly in some cases and implicitly in others.¹⁷ But their general influence can be stated simply. The more intimate the place or thing targeted by surveillance, the more likely it is to violate reasonable expectations of privacy. The greater the amount of information sought, the more likely it is to violate reasonable expectations of privacy. Conversely, the more costly the investigation, the *less* likely it is to violate reasonable expectations of privacy.¹⁸

These principles are interactive; they do not determine cases in isolation. Their various interactions are explained in detail below,¹⁹ but in short, the Court will typically find a Fourth Amendment search only when at least two of the three principles indicate that a reasonable expectation of privacy has been violated. When two principles conflict and the other is indeterminate, intimacy is generally given the most weight, followed by cost.²⁰

These are not iron laws of Supreme Court behavior, but rather practical guidelines to help explain and predict the outcomes of the Court's cases. Yet their explanatory power is substantial. The Court's

¹⁴ *Carpenter*, 138 S. Ct. at 2217–18; *United States v. Jones*, 565 U.S. 400, 413–16 (2012) (Sotomayor, J., concurring); *Jones*, 565 U.S. at 429 (Alito, J., concurring).

¹⁵ See *infra* Sections II.A–.C.

¹⁶ *Id.*

¹⁷ See *id.*; see also *infra* app. tbl.1.

¹⁸ See *infra* Part II.

¹⁹ See *infra* Section II.D.

²⁰ See *infra* Section III.B.

rulings track them in the vast majority of its “reasonable expectation of privacy” decisions to date.²¹ This Article traces the principles of intimacy, amount, and cost back throughout the Court’s Fourth Amendment jurisprudence, providing a coherent account of a body of law thought by many to be incomprehensible.²² It then looks forward, generating testable predictions for future cases and offering a potential means for law enforcement officials to determine how the Fourth Amendment applies in various contexts. Along these lines, it analyzes how the Court is likely to resolve the next wave of cases involving advanced technologies, including drones, “smart” homes, and facial recognition software.

More broadly, the Article gives a theoretical account of the principles and their interactions, synthesizing them into a unified model of Fourth Amendment privacy. The model can bring coherence to the morass of current doctrine and advance scholarly understanding of the reasonable expectation of privacy standard.

The Article concludes by exploring the normative implications of the principles-based approach to Fourth Amendment privacy. Intuitively assessing intimacy, amount, and cost benefits the Court in several ways. For example, these principles act as effective proxies for the privacy harms and potential for abuse associated with government surveillance.²³ The principles-based approach also avoids the serious problems that could arise if the Court resolved cases according to people’s actual expectations of privacy.²⁴

There are, however, notable drawbacks to the Court’s intuitive approach. The Justices’ assessments of intimacy, amount, and cost tend to be haphazard and non-rigorous, and critics have justifiably taken issue with some of the Court’s assertions about these principles.²⁵ Further, setting broad rules based on the intimacy, amount, and cost of a surveillance practice may be problematic because these variables can change dramatically over time, or even from case to case.²⁶

Greater recognition of the principles-based approach would help mitigate some of these drawbacks and would have several additional benefits for courts and other legal actors. The overt analysis of inti-

²¹ See *infra* Part III.

²² See, e.g., Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN’S L. REV. 1149, 1150–51 (1998).

²³ See *infra* Section IV.A.

²⁴ *Id.*

²⁵ See *infra* Section IV.B.

²⁶ *Id.*

macy, amount, and cost would be more tractable for lower courts, would allow courts to use a single conceptual model, and would improve Supreme Court decision-making in future cases. In addition, the model may allow law enforcement officials to better predict when a new surveillance technique will be deemed a Fourth Amendment search.²⁷

The Article proceeds in four parts. Part I recounts the Supreme Court's development of the reasonable expectation of privacy test and reviews scholars' attempts to make sense of it. Part II describes the emerging principles of Fourth Amendment privacy in detail and synthesizes them into a unified explanatory model. Part III applies this model to the Supreme Court's reasonable expectation of privacy cases, finding that the vast majority of such cases are resolved as the principles indicate. Part IV traces the advantages and disadvantages of the principles-based model, and makes the case for greater recognition of the principles. It then applies the model to several frontier issues in Fourth Amendment law, generating predictions as to how the Court will address the next wave of surveillance technologies.

I. THE MYSTERY OF THE FOURTH AMENDMENT'S SCOPE

A. *The Supreme Court and the Katz Test*

The test that primarily governs the Fourth Amendment's scope was developed by Justice Harlan in his solo concurrence in *Katz v. United States*.²⁸ Harlan wrote that the Fourth Amendment's prohibition on unreasonable searches only applied to a person who has "exhibited an actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"²⁹ Harlan's formula was condensed in subsequent cases, with the court effectively finding a search when the government violated an individual's "reasonable expectation of privacy."³⁰

²⁷ See *infra* Section IV.C.

²⁸ 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Supreme Court has recently adopted a subtest that finds a Fourth Amendment search when an official physically touches property for the purpose of gathering information. See *supra* note 1.

²⁹ *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

³⁰ See e.g., *Oliver v. United States*, 466 U.S. 170, 178 (1984) (holding that "a search proscribed by the [Fourth] Amendment" occurs when certain government intrusions "violate[] reasonable expectations of privacy"); *Terry v. Ohio*, 392 U.S. 1, 9 (1968) (noting "wherever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable government intrusion" (citation omitted)).

The Supreme Court has applied this standard in numerous cases since *Katz* was decided. But what makes an expectation of privacy “reasonable” for Fourth Amendment purposes remains ambiguous.³¹ The Court has given several conflicting rationales for its decisions, neglecting to develop any coherent theory that might help legal actors predict the scope of the Fourth Amendment.³² Factors that seem determinative in some surveillance cases are often expressly rejected in others.

For instance, the Court has stated that people reasonably expect privacy in their duffel bags³³ and their friends’ houses³⁴ because the probability of a privacy intrusion is very low. In other cases, by contrast, the Court has expressly rejected the idea that a low probability of intrusion can determine the Fourth Amendment’s scope.³⁵ The upshot is that the “mere expectation . . . that certain facts will not come to the attention of the authorities” is not a reliable indicator that the Fourth Amendment will apply.³⁶

The Court has several times referred to property concepts in determining people’s reasonable expectations of privacy.³⁷ Yet it has also repeatedly rejected the idea that property concepts determine reasonable expectations of privacy, noting that a primary goal of *Katz* was to move beyond such limited conceptions of the scope of the Fourth Amendment.³⁸ Further, the Court has held in several cases that the exposure of information to third parties like telephone companies or banks eliminates any reasonable expectation of privacy in that infor-

³¹ See Kerr, *supra* note 2, at 504.

³² See *id.*; see also *O’Connor v. Ortega*, 480 U.S. 709, 715 (1987) (plurality opinion) (“We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.”).

³³ See *Bond v. United States*, 529 U.S. 334, 338–39 (2000).

³⁴ See *Minnesota v. Olson*, 495 U.S. 91, 96–99 (1990).

³⁵ See, e.g., *Illinois v. Caballes*, 543 U.S. 405, 408–09 (2005) (concluding that the probability of detection by authorities is not determinative of the Fourth Amendment’s scope); *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (“Obviously, however, a ‘legitimate’ expectation of privacy by definition means more than a subjective expectation of not being discovered. A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as ‘legitimate.’”); *United States v. White*, 401 U.S. 745, 751–52 (1971) (plurality opinion) (noting the irrelevance of people’s “actual expectations of privacy” to resolving *White*’s case).

³⁶ *United States v. Jacobsen*, 466 U.S. 109, 122 (1984).

³⁷ See *Rakas*, 439 U.S. at 143 n.12; *United States v. Miller*, 425 U.S. 435, 440 (1976).

³⁸ See, e.g., *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018); *Oliver v. United States*, 466 U.S. 170, 183–84 (1984).

mation.³⁹ Yet, just as often, the Court has ruled that the Fourth Amendment does apply to such information, which remains protected despite its exposure to third parties.⁴⁰ Both lines of precedent remain in force, and the Court has declined to explain when third-party exposure will foreclose Fourth Amendment protection in future cases.⁴¹ Similar contradictions can be observed in cases that alternately rely on or disregard social norms of privacy,⁴² or the steps that citizens take to prevent observation by others.⁴³

This is not to say that there are no consistent principles guiding the Court's Fourth Amendment scope jurisprudence—only that the Court has thus far failed to identify them. The Court's Fourth Amendment rulings are not random. Only a small subset are controversial or widely criticized, despite scholars' widespread condemnation of the *Katz* test in general.⁴⁴ Some stable set of principles or intuitions seems to guide the Court's rulings, even as the Court's reasoning remains a contradictory mess.

B. *The Search for Reasonable Expectations of Privacy*

This Section examines scholars' attempts to bring coherence to the concept of reasonable expectations of privacy. These attempts have met only partial success. Scholars have clarified some aspects of the test and provided helpful accounts of post-*Katz* caselaw. But the

³⁹ See *Smith v. Maryland*, 442 U.S. 735, 744 (1979); *Miller*, 425 U.S. at 442–43; *White*, 401 U.S. at 752.

⁴⁰ See *Carpenter*, 138 S. Ct. at 2223; *Ferguson v. City of Charleston*, 532 U.S. 67, 84–85 (2001); *Stoner v. California*, 376 U.S. 483, 489 (1964).

⁴¹ See *Carpenter*, 138 S. Ct. at 2220 (expressly declining to overrule prior third-party doctrine cases and emphasizing the narrowness of its holding); *id.* at 2223 (declining to apply the third-party doctrine to cell phone location data based on its unique characteristics, including that it was “deeply revealing,” had “depth, breadth, and comprehensive reach,” and was “inescapable and automatic”).

⁴² Compare *Georgia v. Randolph*, 547 U.S. 103, 122–23 (2006) (holding that the police could not lawfully enter a home with the consent of one occupant when the other occupant objected based largely on the social norms of the situation), *with, e.g., California v. Greenwood*, 486 U.S. 35, 40 (1988) (holding that the police may open and look through people's trash bags left out on the sidewalk), *and Miller*, 425 U.S. at 445 (holding that the police may obtain bank records despite powerful norms and explicit agreements against disclosing customer information). See generally *infra* note 53 and accompanying text.

⁴³ Compare *Katz v. United States* 389 U.S. 347, 352 (1967) (emphasizing that *Katz* took steps to protect himself against eavesdropping), *with Florida v. Riley*, 488 U.S. 445, 448–50 (1989) (no reasonable expectation of privacy in a greenhouse in a backyard despite the owner's protecting it with several high fences and a “DO NOT ENTER” sign), *and California v. Ciraolo*, 476 U.S. 207, 213–14 (1986) (no reasonable expectation of privacy in the backyard of a home despite the homeowner enclosing it with high double fences).

⁴⁴ See *supra* notes 10–11.

search for universal principles to guide the reasonable expectations of privacy inquiry has largely come up empty, and the *Katz* test is still widely considered to be vague and unpredictable.⁴⁵ The discussion below reviews some of the most innovative analyses of the reasonable expectation of privacy test.

One of the most influential early accounts of *Katz* can be found in Anthony Amsterdam's 1974 Oliver Wendell Holmes lecture.⁴⁶ Amsterdam described the lack of a "single coherent analytical framework" for the Court's Fourth Amendment decisions and the difficulty of creating such a framework, given the need to regulate police behavior across a wide variety of domains.⁴⁷ Amsterdam also noted that the portion of the *Katz* test that looks to subjective expectations could not be taken literally, lest the government be able to destroy people's Fourth Amendment rights simply by announcing their intrusions before carrying them out.⁴⁸ The Supreme Court later partially adopted this reasoning, noting that the *Katz* inquiry is largely an objective one.⁴⁹ Empirical work on Fourth Amendment cases likewise indicates that the subjective inquiry plays little role in Fourth Amendment scope cases.⁵⁰

In more recent decades, scholars have noted that courts often look to social norms and practices in trying to discern reasonable expectations of privacy.⁵¹ Still, the Supreme Court has "failed to provide guidance" as to how such norms should be assessed or when they are sufficient to establish a reasonable expectation of privacy.⁵² Moreover,

⁴⁵ See, e.g., William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1825 (2016); Amitai Etzioni, *Eight Nails into Katz's Coffin*, 65 CASE W. RES. L. REV. 413, 413–15 (2014); Solove, *supra* note 10, at 1511.

⁴⁶ Amsterdam, *supra* note 10, at 349.

⁴⁷ *Id.* at 350, 369.

⁴⁸ *Id.* at 384.

⁴⁹ See *Hudson v. Palmer*, 468 U.S. 517, 525 n.7 (1984) (noting that the Court "has always emphasized the second of [*Katz*'s] requirements," i.e. the objective prong of the *Katz* test); *Smith v. Maryland*, 442 U.S. 735, 740–741 (1979) (noting that the objective inquiry would prevail over a subjective one in situations where expectations are shaped by government behavior); *supra* note 35.

⁵⁰ Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 116 (2015).

⁵¹ E.g., William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 37 (2001). For early work on tendencies in Fourth Amendment cases, see Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy,'* 34 VAND. L. REV. 1289 (1981).

⁵² Heffernan, *supra* note 51, at 37.

the Court appears to rely on social norms in some cases only to ignore or reject them in others.⁵³

Sherry Colb and other scholars have described the growing importance of the “third-party doctrine,” which provides that individuals generally cannot have a reasonable expectation of privacy in information disclosed to a third party such as a bank or telephone company.⁵⁴ Colb noted that, in its third-party cases, the Court typically treats exposure to one person as exposure to the public, and the risk of exposure as a certainty of exposure.⁵⁵ Nonetheless, Colb identified other cases where the Court appeared to contradict these rules in order to preserve citizens’ privacy, a trend that has intensified in recent cases involving third-party exposure.⁵⁶

Perhaps the most successful descriptive account of the reasonable expectation of privacy test was one that embraced the chaos and contradiction of the Supreme Court’s Fourth Amendment cases. Orin Kerr’s groundbreaking 2007 study described four distinct, conflicting models of Fourth Amendment privacy that the Court uses in various cases.⁵⁷ In some cases, the Court looks to the actual probability of detection or exposure of private information.⁵⁸ In others, it employs a “private facts” model that asks whether the information found by the government was particularly private.⁵⁹ In a third set of cases, the Court looks to other sources of law and finds a search only when the police conduct at issue violates such law.⁶⁰ In a fourth set of cases, the Court engages in policy balancing, weighing the costs and benefits of allowing suspicionless government searches.⁶¹

Kerr described how the Supreme Court ignores or expressly repudiates each of these models in some cases even as it overtly relies on them in others.⁶² He ultimately defended the Court’s use of multi-

⁵³ *Id.* at 81–82, 87. Heffernan notes that police stakeouts, obtaining bank records, and scrutiny of a person’s dialed phone numbers violate social norms of privacy but are nonetheless not considered Fourth Amendment searches.

⁵⁴ Colb, *supra* note 11, at 122; *see also*, e.g., Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 39–40 (2011) (describing the doctrine and predicting its practical demise).

⁵⁵ Colb, *supra* note 11, at 122.

⁵⁶ *See id.* at 160–82; *see also* *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (expressly limiting the reach of the third-party doctrine).

⁵⁷ Kerr, *supra* note 2, at 503.

⁵⁸ *Id.* at 510–12.

⁵⁹ *Id.* at 512–13.

⁶⁰ *Id.* at 516.

⁶¹ *Id.* at 519.

⁶² *Id.* at 508–22.

ple contradictory models, arguing that the complexity of the Fourth Amendment inquiry makes a single theoretical model unattainable.⁶³ This latter position is controversial, and scholars continue to bemoan the unpredictability and lack of theoretical coherence of the multi-model *Katz* approach.⁶⁴ Nonetheless, Kerr's account was a major step forward, helping to clarify and categorize a body of law that had previously appeared to defy categorization.

On a more abstract level, Kerr has also posited that courts in Fourth Amendment cases often react to social or technological changes by attempting to restore the prior balance between law enforcement effectiveness and privacy.⁶⁵ For instance, when white-collar crimes became more prevalent, the Supreme Court permitted the use of warrants to obtain non-contraband evidence and loosened prohibitions on the use of subpoenas.⁶⁶ Although such equilibrium adjustment likely does play a general role in many Fourth Amendment contexts, its application to the Court's reasonable expectation of privacy test may be limited. For example, its application is ambiguous in many situations where a new technology (cars, telephones, computers, etc.) is used by both criminals and the police.⁶⁷ Even when a new technology only helps one side, Kerr does not claim that the general theory of equilibrium adjustment is precise enough to predict Fourth Amendment case outcomes.⁶⁸ Indeed, the theory would have failed to predict the outcomes of many Fourth Amendment cases involving new police practices.⁶⁹ The general concept of equilibrium adjustment

⁶³ *Id.* at 542.

⁶⁴ See, e.g., Solove, *supra* note 10, at 1511; Lior Strahilevitz & Matthew Tokson, *Should Fourth Amendment Law Pay Attention to What People Expect? If So, How?*, CONCURRING OPINIONS (Nov. 27, 2017), <https://web.archive.org/web/20171204041858/https://concurringopinions.com/archives/2017/11/should-fourth-amendment-pay-attention-to-what-people-expect-if-so-how.html> [<https://perma.cc/34XF-JZNT>].

⁶⁵ See Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

⁶⁶ *Id.* at 508–09.

⁶⁷ Ohm, *supra* note 11, at 1341–45.

⁶⁸ See Kerr, *supra* note 65, at 525 (noting that the extent to which courts will adjust in response to a new practice is unclear because the historical baseline that courts measure against is uncertain); *id.* at 500–01 (acknowledging that equilibrium adjustment's impact on a pending Supreme Court Fourth Amendment case is difficult to assess).

⁶⁹ See, e.g., *Illinois v. Caballes*, 543 U.S. 405, 408–09 (2005) (holding that police use of a drug-sniffing dog to inspect a car was not a search); *Florida v. Riley*, 488 U.S. 445, 450 (1989) (holding that the visual inspection of a greenhouse in the backyard of a home from a helicopter was not a search); *California v. Ciraolo*, 476 U.S. 207, 212–13 (1986) (holding that the visual inspection of the backyard of a home from an airplane was not a search); *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986) (holding that detailed aerial inspection of a chemical plant using a sophisticated aerial mapping camera was not a search); *United States v. Karo*, 468 U.S.

can be observed in criminal procedure cases such as those involving subpoenas, infrared scans of houses, and some exceptions to the warrant requirement,⁷⁰ but it is not meant to be a descriptive account of the reasonable expectation of privacy test.

Although the reasonable expectation of privacy test is better understood than it was at the start of the *Katz* era, the Supreme Court's application of the test and the principles that drive it largely remain a mystery. The outcomes of new Supreme Court cases are difficult to predict.⁷¹ Scholars continue to complain about the *Katz* test's theoretical incoherence, unpredictability, and inconsistency in administration.⁷² While many scholars have acknowledged the Supreme Court's use of four models of the *Katz* test, few support a regime of multiple, conflicting models that judges must select from with no overarching theory or norm to guide them.⁷³ Treatises and casebooks continue to struggle to explain the *Katz* test. Most simply report the relevant case outcomes,⁷⁴ and many overtly acknowledge the absence of a coherent theory or stable definition of reasonable expectations of privacy.⁷⁵

Finally, a large portion of Fourth Amendment scholarship has focused on criticizing *Katz* rather than explaining it.⁷⁶ Many scholars

705, 720 (1984) (holding that police use of a tracking beeper to remotely track a car was not a search); *United States v. Knotts*, 460 U.S. 276, 284–85 (1983) (same); *United States v. Place*, 462 U.S. 696, 707 (1983) (holding that police use of a drug-sniffing dog in a public place was not a search). Kerr contends that the *Ciraolo* case reflects equilibrium adjustment in response to *Ciraolo*'s use of a fence, but his argument appears to depend on the debatable claim that fences were a novel innovation that altered the traditional balance of privacy or that airplanes do not themselves substantially increase police surveillance power. See Kerr, *supra* note 65, at 524–25.

⁷⁰ See *id.* at 501, 507–10.

⁷¹ This is true even for judges. For example, in *Carpenter v. United States*, the Court reversed the unanimous holdings of the circuit courts despite those courts' adherence to the principles of previous cases. See 138 S. Ct. 2206, 2223 (2018); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. REV. 139, 161–63 (2016) (describing the circuit court cases).

⁷² See *supra* notes 10–11, 45 and accompanying text.

⁷³ See generally Strahilevitz & Tokson, *supra* note 64 (articulating a familiar critique of the multi-model approach).

⁷⁴ See, e.g., ERWIN CHERMERINSKY & LAURIE L. LEVENSON, *CRIMINAL PROCEDURE: INVESTIGATION* 30–36 (2d ed. 2013); RUSSELL L. WEAVER ET AL., *PRINCIPLES OF CRIMINAL PROCEDURE* 97–108 (5th ed. 2016).

⁷⁵ The current state of confusion and cynicism among casebook and treatise authors is similar to that observed in 2007. See Kerr, *supra* note 65, at 505 (reviewing casebooks' treatments of the *Katz* test); see also RONALD J. ALLEN ET AL., *CRIMINAL PROCEDURE: INVESTIGATION AND THE RIGHT TO COUNSEL* 353–54 (2016) (expressing doubt that there is any overarching theory behind the *Katz* test and emphasizing critiques of the *Katz* regime as a whole); 1 WAYNE R. LEFAVE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* § 2.1(d) (5th ed. 2012) (same).

⁷⁶ See, e.g., Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468, 1473 (1985); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme*

have called for replacing the *Katz* test with a more coherent, predictable, or comprehensive approach.⁷⁷ That may yet be the optimal solution, and there are certainly many criticisms of *Katz* that have little to do with its unpredictability or its lack of a unified theoretical model.⁷⁸ But the Supreme Court has indicated in recent cases that it will continue to use the framework of *Katz* even as it addresses ever more complex surveillance technologies and social practices relevant to privacy.⁷⁹ Further, as the next Part explores, there is reason for optimism that a coherent theory of reasonable expectations of privacy is possible. Intelligible principles have begun to emerge from the chaos of Fourth Amendment caselaw.

II. THE PRINCIPLES OF FOURTH AMENDMENT PRIVACY

This Part explores the emerging principles of Fourth Amendment privacy. As the Supreme Court has applied the reasonable expectation of privacy test in more than 40 cases over the past five decades, patterns have emerged from the resulting body of caselaw. Further, recent cases involving unconventional surveillance technologies have obliged the Justices to identify their fundamental concerns regarding police surveillance. By examining the Court's opinions both old and new, this Article aims to identify consistent, intelligible principles of Fourth Amendment privacy.

Below, I describe three emerging principles of privacy that appear to operate in virtually all Fourth Amendment scope cases: the intimacy of the place or thing targeted by the government; the amount of information sought; and the cost of the investigation. The interaction of these principles is key. For instance, the intimacy of the surveillance at issue generally indicates a Fourth Amendment search only if the amount of data collected or the cost of collection also indicate a search. And the same is true for the other two principles. These are

Court, Technology and the Fourth Amendment, 72 Miss. L.J. 5, 28–29 (2002); Sundby, *supra* note 10, at 1791; *supra* notes 10–11.

⁷⁷ See, e.g., Baude & Stern, *supra* note 45, at 1825; Richard M. Re, *Fourth Amendment Fairness*, 116 MICH. L. REV. 1409, 1409 (2018); Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485, 522 (2014); Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 743–45 (2019); Michael J. Zydney Mannheimer, *The Contingent Fourth Amendment*, 64 EMORY L.J. 1229, 1284–87 (2015).

⁷⁸ E.g., *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring); Colb, *supra* note 11, at 132–39; Ohm, *supra* note 11, at 1325–26; Solove, *supra* note 10, at 1522–24; William Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1021 (1995).

⁷⁹ See *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14, 2227 (2018).

not independent models that appear in some cases and are repudiated in others—they function in virtually every government surveillance context.

This is not to say that the Supreme Court has expressly acknowledged these principles in every Fourth Amendment scope case decided since *Katz*. Nor do the Justices methodically analyze each of these principles as they consider how to rule. Rather, these principles likely shape judicial intuitions regarding the severity of a surveillance practice and the need for constitutional regulation.⁸⁰ These intuitions appear to drive case outcomes in the vast majority of the Court's Fourth Amendment search cases.

Of course, it is possible that the principles strongly correlate with case outcomes without actually causing them. But in any event, the principles provide a useful lens through which to view and analyze Fourth Amendment jurisprudence. Further, while the principles are not always discussed in the Court's opinions, the Court has overtly acknowledged them in a growing number of cases, especially in recent cases involving GPS and cell phone signal tracking.

My synthesis of these principles here draws on prior work by several scholars, many of whom have focused on a single consideration, while others have noted numerous factors that federal and state courts may discuss when resolving Fourth Amendment cases. In particular, Stephen Henderson's analysis of state courts,⁸¹ Susan Freiwald's examination of courts of appeals cases dealing with video surveillance,⁸² and Paul Ohm's detailed study of *Carpenter v. United States*⁸³ helpfully discuss a wide range of considerations that courts have identified as

⁸⁰ Thus, when the government collects a large amount of intimate information at low cost, the Justices are especially likely to identify such surveillance as violating a reasonable expectation of privacy. See *infra* Part III.

⁸¹ See Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 985–1014 (2007).

⁸² See Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, paras. 10, 62–70.

⁸³ 138 S. Ct. 2206 (2018); see Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357 (2019). Ohm argues that the *Carpenter* case essentially reinvented the reasonable expectation of privacy test, implicitly creating a test that examines factors such as the detail and precision of the information obtained, its revealing nature, how frequently the data is collected, how long it has been recorded, the inescapable and automatic nature of its collection, and how many people have been tracked. Although each of these factors may play a role in future cases, the *Carpenter* Court did not expressly modify *Katz*, and it is unlikely that the Court intended to do so implicitly. Indeed, the Court emphasized that “[o]ur decision today is a narrow one,” declined to overrule any prior cases, and expressly listed several Fourth Amendment issues (including several issues closely related to historical cell phone data) on which the Court expressed no opinion. *Carpenter*, 138 S. Ct. at 2220.

important in various surveillance contexts. Building on this literature, this Article's analysis focuses on a more universal set of principles that appear to shape the Justices' intuitions in nearly all Supreme Court cases involving reasonable expectations of privacy. It then combines these principles, describing their interactions in detail and creating a unified model of Fourth Amendment reasonable expectations of privacy.

A. *Intimacy*

The first principle governing Fourth Amendment privacy is intimacy. Specifically, it is the intimacy of the information sought or the place or item examined by the police. Intimacy refers to the personal or sensitive nature of a thing, and to qualities associated with close, familial, or romantic relationships with others.⁸⁴ The inquiry is forward-looking in the surveillance context, focusing on the goal of the surveillance rather than what is actually found.

Intimacy is an important aspect of privacy, one of several foundations of privacy that theorists have identified.⁸⁵ It is also relatively concrete and identifiable. Its core concepts are broadly familiar, as is the importance of relationships and freedom from observation by non-intimates.⁸⁶ Further, privacy theorists have fleshed out the meaning and importance of intimacy in detail, offering a theoretical framework for assessments of intimacy in real-world contexts.⁸⁷ Although intimacy is a longstanding consideration in Fourth Amendment law and the most well-established of the Fourth Amendment principles, the Supreme Court has never given it any doctrinal foundation or explained why intimacy is important. Yet a justification for the role of intimacy is easy to conceive. The more intimate the place or thing targeted by the police for investigation, the more likely such investigation is to infringe the privacy of the affected person or persons. The Court has long considered the home to be the most intimate of places

⁸⁴ See *Intimacy*, THE NEW OXFORD AMERICAN DICTIONARY (2001); JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 75 (1992).

⁸⁵ Other aspects of privacy include control over information, limited access to the self, personal development, and autonomy. See generally Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (detailing various aspects of privacy and describing theories centering on each aspect).

⁸⁶ See INNESS, *supra* note 84, at 61–63.

⁸⁷ See, e.g., *id.* at 74–79 (arguing that the core of the concept of intimacy refers to those behaviors intrinsically motivated by love, affection, or care and often having an expressive element related to that motivation); Robert S. Gerstein, *Intimacy and Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY 265–66 (Ferdinand D. Schoeman ed., 1984) (describing the experiential aspects of intimacy and its importance as a state of being free of observation and judgment).

and has often discussed the private activities that occur therein.⁸⁸ The home accordingly receives the Fourth Amendment's strongest protections.⁸⁹ As the places or information sought by police move further away from the home or from the types of intimate activities traditionally associated with the home, Fourth Amendment law generally offers less protection, holding all else equal.⁹⁰

The Supreme Court has discussed the intimacy of police surveillance since its earliest post-*Katz* cases and in numerous cases since then. In the late 1960s, the Court supported its holding that pat-downs of suspects were Fourth Amendment searches by explaining that such techniques intruded on the "sanctity of the person."⁹¹ The Court would later place intimacy at the core of the Fourth Amendment right, justifying its decision not to extend Fourth Amendment protection to open fields after *Katz* by concluding that "open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance."⁹² In another case, the Court explained that the use of sophisticated camera equipment to surveil commercial property was not a search because "the photographs here are not so revealing of intimate details as to raise constitutional concerns."⁹³ Likewise, the use of a helicopter to surveil a suspect's backyard was not a search in part because the police observation was largely limited to a greenhouse in the backyard and revealed "no intimate details."⁹⁴ Infrared scanning of a home was a search because "[i]n the home, our cases show, *all* details are intimate details."⁹⁵ Finally, in recent cases holding that the Fourth Amendment applies to location tracking on public streets, the Justices have emphasized the potentially revealing nature of such data, which may provide "an intimate window into a person's life."⁹⁶

⁸⁸ See, e.g., *Kyllo v. United States*, 533 U.S. 27, 31, 37 (2001); *Michigan v. Clifford*, 464 U.S. 287, 295 (1984); *Silverman v. United States*, 365 U.S. 505, 511–12 (1961).

⁸⁹ *Kyllo*, 533 U.S. at 31.

⁹⁰ See *Ashdown*, *supra* note 51, at 1303–05.

⁹¹ *Terry v. Ohio*, 392 U.S. 1, 17 (1968).

⁹² *Oliver v. United States*, 466 U.S. 170, 179 (1984). The Court went on to state that "[t]here is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields." *Id.*; see *United States v. Dunn*, 480 U.S. 294, 302 (1987) ("It is especially significant that the law enforcement officials possessed objective data indicating that the barn was not being used for intimate activities of the home.").

⁹³ *Dow Chem. Co. v. United States*, 476 U.S. 227, 238 (1986).

⁹⁴ *Florida v. Riley*, 488 U.S. 445, 452 (1989).

⁹⁵ *Kyllo v. United States*, 533 U.S. 27, 37 (2001).

⁹⁶ *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (citing *Jones v. United States*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). Some state courts have also overtly considered intimacy when deciding cases involving bank records, garbage left for collection, power

Scholars have also discussed the importance of intimacy, though generally in prescriptive rather than descriptive work. Christopher Slobogin has conducted several surveys measuring the perceived “intrusiveness” of various police conduct scenarios.⁹⁷ Intrusiveness differs from intimacy in some ways—it encompasses seizures that do not substantially implicate intimacy, it can be affected by perceptions of whether a search was justified, and it may capture the amount of force used by the police rather than the sensitivity of the information targeted.⁹⁸ Nonetheless, the concepts partially overlap, and, for instance, the police actions rated most invasive nearly always involve targeting intimate places or information, such as the inspection of a bedroom, reading a diary, or a body cavity search.⁹⁹ Slobogin’s surveys can help judges and lawyers more accurately gauge the intimacy of various surveillance practices, an inquiry that at present is largely intuitive. Orin Kerr has discussed what he terms the “private facts” model, used in a subset of Fourth Amendment cases, which considers the privacy of the information that the government collects.¹⁰⁰ This model looks to what the police actually uncover—which is often impossible to predict *ex ante*—rather than what they target. But the concepts are theoretically similar, and Kerr helpfully identifies cases that appear to turn on the intimacy, or lack thereof, of the information sought by the police.¹⁰¹

The Supreme Court’s cases nonetheless reveal that intimacy is not the sole determinant of the Fourth Amendment’s scope. The Court has held that the police can obtain intimate information or target intimate locations without violating reasonable expectations of privacy. For instance, a government informant recording a suspect’s

consumption records, and driver’s license records. *See* State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993); State v. Granville, 142 P.3d 933, 941 (N.M. Ct. App. 2006); Commonwealth v. Duncan, 817 A.2d 455, 463 (Pa. 2003); State v. McKinney, 60 P.3d 46, 51 (Wash. 2002); Henderson, *supra* note 81, at 994.

⁹⁷ *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 (2008); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 275–80 (2002); [hereinafter Slobogin, *Public Privacy*]; Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society,”* 42 DUKE L.J. 727, 738–39 tbl.1. (1993).

⁹⁸ *See* Slobogin & Schumacher, *supra* note 97, at 734–35, 738–39 tbl.1.

⁹⁹ *See id.* at 738–39 tbl.1; *see also* Michael Gentithes, *The End of Miller’s Time: How Sensitivity Can Categorize Third-Party Data After Carpenter*, 53 GA. L. REV. 1039 (2019) (discussing the “sensitivity” of data in the third-party doctrine context).

¹⁰⁰ Kerr, *supra* note 2, at 512–13.

¹⁰¹ *Id.* at 513–14; United States v. Jacobsen, 466 U.S. 109, 123 (1984); United States v. Karo, 468 U.S. 705, 715 (1984).

conversations inside of a house does not constitute a Fourth Amendment search,¹⁰² nor does examining a bag of household trash left on the curb, despite its ability to reveal the intimate activities of the home.¹⁰³ The Court has also held that the collection of non-intimate information can be a search.¹⁰⁴ Yet, as I argue below, the Supreme Court is not ignoring intimacy even in these cases.¹⁰⁵ Rather, these outcomes likely reflect the interaction of intimacy with other principles that drive the reasonable expectation of privacy inquiry. Intimacy always plays a role in the Court's intuitive analyses of Fourth Amendment scope cases, but it is not determinative by itself.

B. Amount

The second principle governing Fourth Amendment privacy involves the amount of information sought. In theory, this could be represented by the number of bits of information sought by the police.¹⁰⁶ In practice, the amount of information sought will typically be measured by the extent and duration of a surveillance practice, or how much information about a suspect is ultimately obtained and stored.¹⁰⁷ In most cases, the amount sought and the amount obtained will be the same, and I use the terms interchangeably.

The relevance of the amount of information gathered to privacy is fairly straightforward, and the Supreme Court has begun to overtly analyze this relationship in recent cases. In general, the more information that is collected, the greater the potential for intrusion on the target's privacy. The Court hinted at the importance of the amount of data collected in 1983, when it emphasized the small amount of information gathered by a drug-sniffing dog.¹⁰⁸ In a case decided that same year holding that the "limited use" of an automobile tracking beeper for several hours was not a search, the Court suggested that a program

¹⁰² *United States v. White*, 401 U.S. 745, 752–54 (1971) (plurality opinion).

¹⁰³ *California v. Greenwood*, 486 U.S. 35, 41–42 (1988).

¹⁰⁴ *See, e.g., Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 616 (1989); *Arizona v. Hicks*, 480 U.S. 321, 321 (1987).

¹⁰⁵ *See infra* Section II.D; *infra* Part III.

¹⁰⁶ A bit of information is a binary value of either zero or one, which when combined with other bits can be used to represent all types of information. For instance, digital information is stored in bits, but can represent and store detailed lexical, visual, auditory, and other types of information.

¹⁰⁷ Information obtained during the course of an investigation that is wholly orthogonal to the suspect or the investigation is not counted in this calculus. Thus, the visual appearance of a sunset or some fluffy clouds observed by police officers while they tail a suspect would not be counted as part of the relevant data collected by the investigation.

¹⁰⁸ *United States v. Place*, 462 U.S. 696, 707 (1983).

of constant surveillance of citizens might constitute a search, presumably because such voluminous surveillance would raise far greater privacy concerns.¹⁰⁹

Three decades later, the Court actually was confronted with technologies that allowed the police to track citizens' movements for months at a time. In the location tracking cases, the Court has come to overtly recognize the importance of the quantity of information gathered to Fourth Amendment privacy. In 2012's *United States v. Jones*,¹¹⁰ Justice Alito's concurrence—supported by four other Justices—recognized that long-term surveillance that “secretly monitor[ed] and catalogue[d] every single movement of an individual's car for a very long period” violated reasonable expectations of privacy in a way that briefer, lower-quantity methods of surveillance did not.¹¹¹ And in the recent landmark case *Carpenter*, the Court officially adopted this reasoning, citing Justice Alito's *Jones* concurrence and holding that tracking a cell phone for at least seven days constitutes a Fourth Amendment search.¹¹² The Court noted that the government had “obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.”¹¹³ It repeatedly emphasized the dangers that such a volume of data posed to a citizen's privacy, because it provided an “all-encompassing record of the [cell phone] holder's whereabouts” and could effectively tail a person “every moment of every day for five years” with current technology.¹¹⁴ The Court distinguished previous third-party doctrine cases because those cases involved the collection of a far smaller amount of data: “[T]his case is not about ‘using a phone’ or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.”¹¹⁵ The Court expressly recognized the importance

¹⁰⁹ *United States v. Knotts*, 460 U.S. 276, 284 (1983).

¹¹⁰ 565 U.S. 400 (2012).

¹¹¹ *Id.* at 430 (Alito, J., concurring). Five Justices endorsed Justice Alito's concurrence, although Sotomayor did not officially join it. *See id.* at 413 (Sotomayor, J., concurring).

¹¹² *Carpenter v. United States*, 138 S. Ct. 2206, 2215–17 & n.3 (2018) (“Since GPS monitoring of a vehicle tracks ‘every movement’ a person makes in that vehicle, the concurring Justices concluded that ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy’—regardless whether those movements were disclosed to the public at large.” (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring))).

¹¹³ *Id.* at 2212.

¹¹⁴ *Id.* at 2217–18.

¹¹⁵ *Id.* at 2220.

of the amount of data collected; indeed, the concept played a decisive role in one of the most important Fourth Amendment cases of the last 50 years.

Moreover, there is evidence from outside of Fourth Amendment law that the Court appreciated the importance of amount long before the *Jones* and *Carpenter* cases were decided. In a 1977 case addressing the constitutionality of a state database of prescription drug users, the Court expressly noted “the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”¹¹⁶ In 1989, the Court held that FBI rap sheets collecting publicly available criminal conviction information could not be disclosed under FOIA, because the collection and storage of so much information in one place raised substantial privacy concerns.¹¹⁷ These cases, along with the early *Katz*-test cases mentioned above,¹¹⁸ suggest that the Court has long been attentive to the amount of information gathered by government officials.

There is, in addition, a more subtle relationship between the amount of data collected and privacy. Large aggregations of data can often reveal more than the sum of their parts, by allowing the observer to identify patterns in a surveillance target’s behaviors and to draw revealing connections between disparate sources of information. As Justice Sotomayor recognized in her concurrence in *United States v. Jones*, a large database of an individual’s public movements “reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”¹¹⁹ The government can mine such a record for revealing patterns or links “years into the future.”¹²⁰ Relatedly, the combination of information about a person’s Facebook friends and Amazon purchases might reveal to observers a variety of other information about that person’s life, including their sexual orientation or medical status.¹²¹

116 *Whalen v. Roe*, 429 U.S. 589, 605 (1977). *See id.* at 607 (Brennan, J., concurring) (“The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.”).

117 *U.S. Dep’t of Justice v. Reporter’s Comm. for Freedom of the Press*, 489 U.S. 749, 764, 770 (1989).

118 *See supra* notes 108–11 and accompanying text.

119 *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

120 *Id.*

121 *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, *FORBES* (Feb. 16, 2012, 11:02 AM), <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#3c569b666686> [https://perma.cc/29G8-UGGM]; Ben Tinker, *How Facebook ‘Likes’ Predict Race, Religion, and Sexual*

Many scholars have raised concerns about data aggregation and the potential for abuse that is inherent in large, permanent databases of information about individuals.¹²² David Gray and Danielle Citron have argued that the large quantity of data that new surveillance technologies can collect should lead courts to require a warrant before such technologies can be used at all.¹²³ More broadly, some scholars have suggested that collecting a large quantity of information may substantially invade privacy even when collecting a small quantity of the same type of information does not, a concept sometimes referred to as the “mosaic theory.”¹²⁴ Theorists have debated whether the mosaic theory is a desirable framework for questions of privacy and the Fourth Amendment’s scope.¹²⁵ Although the academic debate is ongoing, the Justices have repeatedly endorsed the idea that the amount of information gathered is relevant to reasonable expectations of privacy.¹²⁶

Nonetheless, there is little in the existing Fourth Amendment literature tracing the importance of amount in the Supreme Court’s reasonable expectation of privacy cases, especially cases decided before *United States v. Jones*. Perhaps that is because it is clear that the amount of data collected is not the sole determinant of the Fourth Amendment’s scope.¹²⁷ For instance, the Court has repeatedly found that the collection of small amounts of data can be a Fourth Amendment search.¹²⁸ In other cases, it has held that obtaining large amounts

Orientation, CNN (Apr. 11, 2018, 1:42 PM), <https://www.cnn.com/2018/04/10/health/facebook-likes-psychographics/index.html> [<https://perma.cc/582M-HQKM>].

¹²² See, e.g., Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1056 (2016); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1112, 1154 (2002).

¹²³ David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 72 (2013).

¹²⁴ *Id.* at 90.

¹²⁵ See *id.* at 101–03 (advocating for a bright-line approach to regulating the use of surveillance technologies); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 343–53 (2012) (arguing that the mosaic theory is difficult to administer properly and could interfere with statutory regulation of government surveillance).

¹²⁶ See *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018); *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *Jones*, 565 U.S. at 430–31 (Alito, J., concurring). Likewise, recent lower court decisions applying *Carpenter* have distinguished it solely on the basis of the amount of information gathered. See, e.g., *Sims v. State*, 569 S.W.3d 634, 646 (Tex. Crim. App. 2019).

¹²⁷ See *infra* Section III.B for a discussion of the role that amount plays in the Supreme Court’s reasonable expectation of privacy cases.

¹²⁸ See, e.g., *Ferguson v. City of Charleston*, 532 U.S. 67, 84–86 (2001) (holding that a state hospital’s testing of pregnant woman’s urine for cocaine was a search); *Bond v. United States*, 529 U.S. 334, 336–39 (2000) (holding the unwarranted inspection of an opaque bag containing a

of information is not a search.¹²⁹ In *Dow Chemical Co. v. United States*,¹³⁰ for example, it held that the government's use of an aerial mapping camera to take detailed photographs of a large chemical facility did not violate any reasonable expectations of privacy.¹³¹

Although the amount of information sought shapes Justices' intuitions in virtually every Fourth Amendment scope case, it is the interaction of amount with other principles such as intimacy that drives case outcomes. In cases where the collection of a small amount of information was held to be a search, the information collected was generally intimate or located in an intimate place.¹³² In *Dow Chemical*, by contrast, the information sought was especially non-intimate, involving the exterior of a chemical plant photographed from over one thousand feet overhead.¹³³ The amount of data gathered guides judicial intuition in the Court's Fourth Amendment scope cases, but it can be counterbalanced by other principles.

C. Cost

The third principle governing Fourth Amendment privacy involves the cost of the surveillance. The Supreme Court likely assesses the costs of surveillance informally and inexactly. The Justices may, for example, consider the time and effort required for police officers to effectuate a surveillance practice; the expense of operating or renting a vehicle or device used in the surveillance; or the difficulty, unpleasantness, or risk to officers of a procedure.¹³⁴ Cost is likely to be most salient to the Court when it is particularly high or particularly low.

This inquiry may consider both the total cost of the surveillance and its unit cost, *i.e.*, the cost per bit of information sought.¹³⁵ When

"brick" of methamphetamine was a search); *Terry v. Ohio*, 392 U.S. 1, 30 (1968) (holding that the physical pat-down of the outside of a suspect's jacket in order to detect weapons was a search).

¹²⁹ *E.g.*, *United States v. Karo*, 468 U.S. 705, 720 (1984) (finding that monitoring a tracking beeper in a car that traveled to various locations was not a search); *United States v. Payner*, 447 U.S. 727, 732 (1980) (holding that seizing several bank documents is not a search); *United States v. White*, 401 U.S. 745, 751–52 (1971) (plurality opinion) (finding that the recording of several conversations by an undercover law enforcement official was not a search).

¹³⁰ 476 U.S. 227 (1986).

¹³¹ *Id.* at 239.

¹³² *See supra* note 129.

¹³³ *See Dow Chemical*, 476 U.S. at 229.

¹³⁴ *See, e.g.*, *California v. Ciraolo*, 476 U.S. 207, 209–10, 213–14 (1986) (discussing a police officer's chartering of a private airplane in order to surveil suspected marijuana growers).

¹³⁵ The total cost of gathering the information would include the average fixed cost plus the marginal cost of the surveillance. In most cases, the average fixed cost will be low and difficult to

the unit cost of surveillance is low, the government can gather a large amount of information at a relatively low cost, raising concerns about privacy and the legitimacy of the surveillance. Forms of surveillance that are scalable and easily applied to large groups of citizens are of particular concern.

Cost is an important component of reasonable expectations of privacy because it impacts both the extent and the validity of government surveillance. Part of this is already partially captured by the principle of amount—as the cost of surveillance decreases, the government becomes more likely to capture greater quantities of information about an individual suspect. Decreases in surveillance costs can also reveal what was once practically obscure, either by making it possible to gather data that would have been prohibitively costly to obtain, or by revealing information (like the infrared heat signature of a house) that may have been difficult to obtain at any price with previous technologies. As practical barriers to government observation are eliminated by new, low-cost surveillance methods, the potential for exposure of private information to the government sharply increases.

The effects described above concern the potential for enhanced surveillance of a particular suspect. But the effects of low-cost surveillance are also concerning when considered on a broader scale. For instance, low-cost surveillance allows the police to monitor a large number of people, most of whom have a very low likelihood of being involved in criminal activity.¹³⁶ Whereas previously the police were likely to engage only in those searches that were worth the relatively high cost, cheaper surveillance technologies greatly increase the probability that innocent persons will be subject to surveillance and its related harms.¹³⁷ Indeed, evidence from low-cost video monitoring in England suggests a higher probability of abuse. Many of the crimes detected by CCTV are low-level crimes that are prone to discriminatory enforcement, such as loitering or underage smoking.¹³⁸ A substantial portion of law enforcement interventions involve removing

quantify, and the marginal cost will be the practically relevant measure. In cases involving multiple potential searches and/or seizures, the marginal cost of each potential search or seizure analyzed by the Court will be the relevant marginal cost.

¹³⁶ See Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477, 521 (2007) (raising concerns about the chilling effects of mass surveillance).

¹³⁷ For a discussion of this effect in the context of the warrant requirement, see Max Minzner & Christopher M. Anderson, *Do Warrants Matter?*, 9 REV. L. & ECON. 169, 192 (2013). For a detailed discussion of the harms of government surveillance, see Tokson, *supra* note 77.

¹³⁸ Slobogin, *Public Privacy*, *supra* note 97, at 247–48.

homeless persons or groups of teenagers from commercial areas despite the absence of any crime at all.¹³⁹ In many public places, the primary impact of low-cost surveillance is often the exclusion of disfavored groups, rather than the deterrence or apprehension of criminals.¹⁴⁰

High-cost surveillance is more likely to be narrowly applied. It is also more likely to be limited to situations that are especially likely to yield evidence of criminal activity.¹⁴¹ Police departments are motivated to solve crimes, and resource-constrained departments are, all else equal, likely to choose the most promising investigations to pursue.¹⁴² In addition, costly surveillance is less prone to abuse because of its greater budgetary and political salience. The greater the expenditure, the more likely it is to come to the attention of some electorally accountable person or entity.¹⁴³ Police are more likely to be required to justify high or unusual expenditures, and potential abuses of surveillance power are more likely to be exposed. Thus, the cost of surveillance is linked to its probable legitimacy. Low-cost surveillance is conducive to government abuses and the widespread surveillance of innocent persons.

For all of these reasons, low-cost surveillance intuitively raises concerns about the government violating reasonable expectations of privacy. Yet cost is probably the least-recognized Fourth Amendment principle in the Supreme Court's Fourth Amendment caselaw. Nonetheless, the Supreme Court has expressly acknowledged the importance of cost in recent decisions involving new technologies that decrease the costs of surveillance.

Several Justices discussed the impact of low-cost surveillance on privacy in concurring opinions joined by a majority of the Justices in *United States v. Jones*. Justice Alito described how new, low-cost surveillance techniques had eroded the structural barriers that had once made pervasive government surveillance "difficult and costly."¹⁴⁴ Previously, "[o]nly an investigation of unusual importance could have justified . . . [the] expenditure of law enforcement resources" necessary

¹³⁹ *Id.* at 248.

¹⁴⁰ *Id.*

¹⁴¹ See *United States v. Jones*, 565 U.S. 400, 429 (2012) (Alito, J., concurring).

¹⁴² See Aziz Z. Huq, *Agency Slack and the Design of Criminal Justice Institutions*, in *THE ROUTLEDGE HANDBOOK OF CRIMINAL JUSTICE ETHICS* (Jonathan Jacobs & Jonathan Jackson eds., 2017).

¹⁴³ Cf. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring) (noting that "limited police resources and community hostility" act as a constraint on police abuses).

¹⁴⁴ *Id.* at 429 (Alito, J., concurring in the judgment).

to track someone's location for several weeks.¹⁴⁵ But new technologies had made it "relatively easy and cheap," and therefore more likely to be widely used.¹⁴⁶ Justice Sotomayor expressed concern that GPS tracking was "low cost" and so "cheap in comparison to conventional surveillance techniques" that it would evade "the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility."¹⁴⁷ The Court later echoed these concerns in *Carpenter*.¹⁴⁸ It stressed that cell phone tracking allowed the government to "effortlessly compile[]" detailed information about an individual, at "practically no expense."¹⁴⁹ As with GPS tracking, cell phone tracking raised serious privacy concerns because it is "remarkably easy, cheap, and efficient compared to traditional investigative tools."¹⁵⁰

The Court's overt recognition of cost in Fourth Amendment cases is relatively new, but there is evidence that the Court has been sensitive to the costs of surveillance since even before *Katz*. In a 1948 case where a government official ordered an automobile passenger to reveal the contents of his pockets, the Court concluded that the Fourth Amendment was designed "to place obstacles in the way of a too permeating police surveillance," a conception of the Amendment that frames cost as a primary bulwark against widespread government monitoring.¹⁵¹ The Court also recognized the importance of cost as a structural protection for privacy in the 1989 case *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*,¹⁵² where it found a "vast difference" between scattered public records that could only be obtained at great cost and a compilation that could be cheaply acquired with a simple FOIA request.¹⁵³ The fact that the information had become available at low cost "alter[ed] the privacy interest implicated by disclosure of that information."¹⁵⁴ As the cost of obtaining the information decreased, the threat to privacy increased, such that FOIA ultimately barred its disclosure.¹⁵⁵

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ *Id.* at 416 (Sotomayor, J., concurring) (internal quotation marks omitted).

¹⁴⁸ *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018).

¹⁴⁹ *Id.* at 2216, 2218.

¹⁵⁰ *Id.* at 2218.

¹⁵¹ *United States v. Di Re*, 332 U.S. 581, 595 (1948) (holding that the search of a car passenger's pockets was not justified on the basis of probable cause to search the car).

¹⁵² 489 U.S. 749 (1989).

¹⁵³ *Id.* at 764.

¹⁵⁴ *Id.*

¹⁵⁵ *See id.*

A handful of scholars have advocated for greater recognition of the importance of surveillance costs. In the context of privacy law, Harry Surden described the presence of structural constraints that prevent surveillance but which are vulnerable to elimination by new technologies.¹⁵⁶ Surden argued that policymakers should intervene to regulate new surveillance technologies that undermine prior structural constraints on surveillance.¹⁵⁷ Kevin Bankston and Ashkan Soltani examined cost in the Fourth Amendment context of location surveillance.¹⁵⁸ They helpfully calculated and compared the costs of various methods of location surveillance in public places, ranging from foot pursuit to car pursuit to cell phone signal tracking.¹⁵⁹ They posited that when a new surveillance technique decreases the marginal cost of observation by a factor of ten or more, that technique is likely to violate a reasonable expectation of privacy.¹⁶⁰

Bankston and Soltani did not examine Supreme Court cases beyond those dealing with novel location tracking technologies, and their descriptive claim is limited to cases where the cost of surveillance drops dramatically.¹⁶¹ Yet their work represents a substantial step towards quantifying the cost of information gathering and demonstrating its relevance to expectations of privacy. Of course, the cost of surveillance is not the sole determinant of outcomes over the fifty-year span of the Supreme Court's post-*Katz* caselaw. The Court has often ruled that costly surveillance is a Fourth Amendment search, and that low-cost surveillance is not. For example, investigations that require substantial police time and effort have been held to be searches, as when officials travel to an office building and search an office,¹⁶² or when arson investigators search a fire-damaged home.¹⁶³ In other cases, low-cost investigations such as dog sniffs,¹⁶⁴ removing

¹⁵⁶ Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1607–08 (2007).

¹⁵⁷ *Id.* at 1619.

¹⁵⁸ See Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* *United States v. Jones*, 123 YALE L.J. 335, 338–39 (2014). Bankston and Soltani also draw general inspiration from Orin Kerr's theory of equilibrium adjustment and Paul Ohm's proposal that courts adjust the law so that solving a crime takes roughly as long with new technologies as it did with prior technologies. See Kerr, *supra* note 65, at 480; Ohm, *supra* note 11, at 1352.

¹⁵⁹ Bankston & Soltani, *supra* note 158, at 350.

¹⁶⁰ *Id.* at 337.

¹⁶¹ See *id.*

¹⁶² *Mancusi v. Deforte*, 392 U.S. 364, 365–66 (1968).

¹⁶³ *Michigan v. Clifford*, 464 U.S. 287, 299 (1984).

¹⁶⁴ *Illinois v. Caballes*, 543 U.S. 405, 409 (2005).

plastic bags from a damaged package,¹⁶⁵ asking the phone company to record a customer's dialed phone numbers,¹⁶⁶ and shining a flashlight into a car¹⁶⁷ did not violate reasonable expectations of privacy. Plainly, cost is not the only consideration at issue in the Court's Fourth Amendment cases.

This Article contends that cost nonetheless influences virtually every Fourth Amendment scope case, even when it is not determinative. Cost interacts with and mediates the other principles of Fourth Amendment privacy. When surveillance is costly, that high cost can mitigate the harms that would normally be caused by the collection of substantial amounts of intimate data. Low-cost surveillance can exacerbate those harms. The next Section further explores the relationship between the Fourth Amendment principles described above, and develops a formal, unified model of Fourth Amendment reasonable expectations of privacy.

D. A Unified Model of Fourth Amendment Privacy

The previous Sections identified three important principles of Fourth Amendment privacy, outlined their theoretical foundations, and described their gradual emergence in the Supreme Court's jurisprudence.¹⁶⁸ This Section brings the emerging Fourth Amendment principles of intimacy, amount, and cost together into a single model. These principles appear to drive the Supreme Court's Fourth Amendment cases by shaping the Justices' intuitions about privacy—but they do so only in combination. By studying how these principles interact, observers can better explain existing cases and predict future outcomes.

I will start with the basic principles described above and then address their interactions. In general, the more intimate the information sought or the place or thing inspected, the more likely it is to violate reasonable expectations of privacy.¹⁶⁹ The greater the amount of information obtained, the more likely it is to violate reasonable expectations of privacy.¹⁷⁰ The greater the cost of the surveillance, the *less* likely it is to violate reasonable expectations of privacy.¹⁷¹

¹⁶⁵ *United States v. Jacobsen*, 466 U.S. 109, 111, 126 (1984).

¹⁶⁶ *Smith v. Maryland*, 442 U.S. 735, 736, 745–46 (1979).

¹⁶⁷ *Texas v. Brown*, 460 U.S. 730, 733, 744 (1983).

¹⁶⁸ *See supra* Sections II.A–.C.

¹⁶⁹ *See supra* Section II.A.

¹⁷⁰ *See supra* Section II.B.

¹⁷¹ *See supra* Section II.C.

These principles operate on an intuitive level, and their interactions cannot be precisely quantified. Yet it may be helpful to approach the principles' interactions in the abstract before giving a more pragmatic account of their interactions.

Setting aside questions of both units and weight, we might represent the basic interaction of these three principles as the intimacy and amount of surveillance minus its cost. When $\text{intimacy} + \text{amount} - \text{cost}$ is too high, then a reasonable expectation of privacy has been violated. A search, thus, occurs whenever $\text{intimacy} + \text{amount} - \text{cost} > \text{a threshold for unacceptable threats to privacy}$.

Further, we could give weights to each of the variables to represent their relative importance in shaping judicial perceptions. Intimacy, for instance, may be more influential than amount and would need to be weighted accordingly.¹⁷² So we might say that a search occurs when $xI + yA - zC > \theta$, where x , y , and z are the weights we accord to the variables.

If we could quantify intimacy, amount, cost, and their weights in various cases, we could eventually generate a numerical value that represents a reasonable expectation of privacy. But few or none of these variables can be precisely quantified, and there is, alas, no mathematical formula for the Fourth Amendment. Nonetheless the conceptual framework developed in this Article is a powerful tool for understanding the Supreme Court's Fourth Amendment scope cases. It can help untangle the "mess"¹⁷³ of the post-*Katz* cases, enabling judges, lawyers, and even laypeople to better understand the reasonable expectation of privacy test. Moreover, by examining the Court's cases in light of the framework, one can identify clear and predictive guidelines that correlate with outcomes in the vast majority of cases.¹⁷⁴ The remainder of this Section describes these guidelines, while Part III examines how they operate in the Supreme Court's post-*Katz* Fourth Amendment cases.

Based on the above account, when the government seeks to obtain intimate information in large amounts and does so at a low cost, judges will find that reasonable expectations of privacy have been violated.¹⁷⁵ Likewise, when the government seeks non-intimate information in small amounts at high cost, judges will find no violation of

¹⁷² See *infra* Section III.B.

¹⁷³ Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 20 (1988).

¹⁷⁴ See *infra* Part III.

¹⁷⁵ See *infra* Section III.A.1.

reasonable expectations of privacy.¹⁷⁶ These are clear cases under this Article's framework, and indeed there is no Supreme Court *Katz* test case that violates this rule in either direction, per the case analysis described in Part III.¹⁷⁷

What about when the principles point in opposing directions? For instance, a government investigation into a computer system might seek intimate information at a low cost but may seek to gather only a small amount of such information. As a general guideline, when the principles point in opposing directions, judges will tend to rule according to the majority of the principles.¹⁷⁸ Thus, in the computer system example, the court would likely hold that the investigation violated reasonable expectations of privacy. This norm is followed in the vast majority of post-*Katz* Supreme Court cases.¹⁷⁹

In rare situations, two principles will point in opposing directions while the third does not indicate an outcome, perhaps because the intimacy, amount, or cost at issue is neither notably high nor low relative to other potential searches. These cases require a consideration of the relative importance of the principles. In practice, intimacy appears to be the most influential principle, followed by cost, with amount as the least influential principle. Accordingly, as a rule of thumb, when intimacy and another principle point in opposing directions and a third principle is roughly neutral, then intimacy will determine the outcome of the case.¹⁸⁰ In cases where intimacy appears roughly neutral, then the cost of the surveillance will generally determine the outcome of the case.¹⁸¹ These are necessarily imprecise norms, although no Supreme Court case decided since *Katz* appears to contradict them.¹⁸²

The above guidelines are not intended to be iron laws of judicial behavior. It is easy, for example, to imagine cases where courts could violate the guidelines even while adhering to the broader conceptual framework. For instance, an especially strong indicator under one principle might outweigh multiple weak indicators that point in the other direction.¹⁸³

¹⁷⁶ See *infra* Section III.A.1.

¹⁷⁷ See *infra* Section III.A.1; app. tbl.1.

¹⁷⁸ See *infra* Section III.A.1.

¹⁷⁹ See *infra* Part III.

¹⁸⁰ See, e.g., *Kyllo v. United States*, 533 U.S. 27 (2001); *Minnesota v. Olson*, 495 U.S. 91 (1990).

¹⁸¹ See *New York v. Class*, 475 U.S. 106, 112–19 (1986).

¹⁸² See *infra* app. tbl.1.

¹⁸³ See *infra* text accompanying notes 263–64. In addition, the direction and magnitude of

Nonetheless, the framework developed here represents a significant step toward understanding the Supreme Court's Fourth Amendment cases and effectively predicting future case outcomes. As Part III details, the framework can help explain the vast majority of Supreme Court decisions involving reasonable expectations of privacy, including several cases that scholars have struggled to explain under existing conceptions of the *Katz* test.

III. EXPLAINING REASONABLE EXPECTATIONS OF PRIVACY

The principles described above appear to shape the outcomes of the Supreme Court's Fourth Amendment scope cases. Yet the Justices do not methodically calculate the intimacy, amount, and cost of surveillance in each case. Rather, these principles likely drive the Justices' intuitions about the severity of a government intrusion on citizens' privacy. By carefully examining the Supreme Court's *Katz* test cases, this Part aims to demonstrate the general role that the principles of intimacy, amount, and cost play in Fourth Amendment law.

As detailed above, the Court has acknowledged the importance of one or another of the principles in various cases, but it has usually addressed only one principle at a time. Overt judicial recognition of the combination of the principles has been rare, although the Court has inched closer to acknowledging them in recent cases. Justice Sotomayor has come the closest in a single, prescient line in her concurrence in *United States v. Jones*. She notes that GPS monitoring is such a threat to privacy because, "by making available at a relatively low cost such a substantial quantum of intimate information . . . [it] may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"¹⁸⁴ Unfortunately her opinion does not elaborate any further, but it correctly identifies the government's collection of a substantial quantity of intimate information at low cost as the quintessential privacy violation, one so serious that it

the various principles may be difficult to calculate precisely. Even a "neutral" indicator that is neither especially high nor low relative to other potential searches may point slightly in one direction or another and may thereby influence judges. Moreover, judicial perceptions of the principles may change over time as societal norms and practices change. The potential for reasonable expectations of privacy to degrade over time as surveillance becomes more common is a well-known criticism of the *Katz* test, and one that is no less applicable to the descriptive framework offered here. *E.g.*, Teri Dobbins Baxter, *Low Expectations: How Changing Expectations of Privacy Can Erode Fourth Amendment Protection and a Proposed Solution*, 84 TEMP. L. REV. 599, 613 (2012).

¹⁸⁴ *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011)).

threatens to undermine democratic society. The *Carpenter* majority opinion is less clear about identifying a synthesis of the three principles, but it does mention all three in a single paragraph, stating that cell phone tracking “contravenes” reasonable expectations of privacy because it can “provide[] an intimate window into a person’s life” and “the Government can access . . . [a] deep repository of historical location information at practically no expense.”¹⁸⁵ The Court is slowly moving towards recognition of the principles as a central determinant of reasonable expectations of privacy.

Still, the majority of Supreme Court cases applying the *Katz* test mention at most one of the principles, and many do not mention them at all. There has been no overt judicial effort to follow the framework described in Section II.D. Yet, at least at the Supreme Court level, compliance with the practical guidelines set out above has been remarkably consistent. No matter which rationale the Court purports to use—positive law, probability, the third-party doctrine, etc.—the majority of Justices find a search when the three principles point in that direction and find no search when they point the other way.

This Part posits that Fourth Amendment scope law is not, at its core, an incomprehensible tangle of conflicting approaches, but rather reflects the intuitive application of the intimacy, amount, and cost model in the vast majority of cases. This analysis largely focuses on the Supreme Court’s Fourth Amendment scope cases rather than those of lower courts. This is not solely because of the greater importance of the Court’s cases. Lower courts are bound by the *Katz* test as written, and are more likely to attempt to apply it literally.¹⁸⁶ By contrast, the Supreme Court is better able to reach outcomes that track its intuitions about privacy, even though it has, thus far, struggled to articulate a consistent rationale for those outcomes.

A. *Reasonable Expectations of Privacy at the Supreme Court*

Since 1967, the Supreme Court has applied the reasonable expectation of privacy test in 41 cases, several of which involved multiple alleged searches.¹⁸⁷ In total, the Court issued 50 rulings on Fourth

¹⁸⁵ *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018).

¹⁸⁶ See Tokson, *supra* note 71, at 154, 156–58, 161–63 (giving examples of lower courts attempting to determine societal expectations of privacy).

¹⁸⁷ This set was limited to cases in which the Court issued a clear ruling as to whether an act of surveillance was a Fourth Amendment search; unspoken or uncontested assumptions were not included. The set includes *United States v. Jones*, where five Justices agreed that the GPS tracking at issue violated reasonable expectations of privacy, although the majority opinion resolved the case by creating an alternative test that finds a search whenever the police physically touch a

Amendment searches in these cases.¹⁸⁸ Four coders separately read and analyzed each of these cases.¹⁸⁹ The coders each assessed the approximate magnitude of the intimacy, amount, and cost of the surveil-

person, house, paper, or effect for the purpose of gathering information. 565 U.S. at 411. It does not include cases applying the “physical touching” test that are not accompanied by separate opinions joined by at least five Justices concluding that reasonable expectations of privacy were violated under the *Katz* test. The omitted physical touching cases are *Florida v. Jardines*, 569 U.S. 1, 4 (2013), and *Grady v. North Carolina*, 135 S. Ct. 1368 (2015) (per curiam). The set also does not contain three special needs cases in which the conclusion that a urine test was a Fourth Amendment search was unspoken or uncontested by the parties and the Justices. See *Chandler v. Miller*, 520 U.S. 305, 314 (1997); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995); *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665 (1989). Nor does it include *Sibron v. New York*, 392 U.S. 40 (1968), a companion case to *Terry v. Ohio*, 392 U.S. 1 (1968), that did not make a *Katz*-test ruling. *Alderman v. United States*, 394 U.S. 165 (1969), was excluded because the Court remanded to the district court for a determination of whether Fourth Amendment rights were violated.

¹⁸⁸ See *supra* note 12; *infra* app. tbl.1.

¹⁸⁹ The coders included the author and three law students who had completed a course in Criminal Procedure. The student coders were not instructed on the model described above. Excluding the author’s codes from the project would yield similar results, albeit with slightly more outlier cases. Conversely, excluding the students’ codes and relying on the author’s coding alone would yield somewhat similar results and slightly more outlier cases. The best results were achieved with a larger and more experientially diverse group of coders. As reported below, using the average values of intimacy, amount, and cost calculated by all four coders, the intimacy, amount, and cost model produced 49 predicted outcomes and one inconclusive outcome. The model’s predicted outcome correlated with the outcome of 46 of 49 (94%) corresponding Supreme Court search decisions. See *supra* Sections III.A–B; *infra* app. tbl.1. Using only the students’ codes, the model would correlate with 43 of 50 (86%) corresponding Supreme Court decisions. Using only the author’s codes, the model would correlate with 45 of 50 (90%) corresponding Supreme Court decisions. Under all of these scenarios, the model’s correlations with case outcomes were statistically significant at the .001 level.

The additional outliers in the students-only results would be *Minnesota v. Olson*, 495 U.S. 91 (1990), *Hudson v. Palmer*, 468 U.S. 517 (1984), *Katz v. United States*, 389 U.S. 347 (1967), one of the decisions in *Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602 (1989) (assessing blood tests administered to railroad employees), and one of the decisions in *New York v. Class*, 475 U.S. 106 (1986) (assessing a police officer’s brief entry into a car). *Arizona v. Hicks*, 480 U.S. 321 (1987), would not be an outlier using the students’ codes alone, although it is in the four-coder results. The additional outliers in the author-alone results would be *Smith v. Maryland*, 442 U.S. 735 (1979), and one of the decisions in *United States v. Karo*, 468 U.S. 705 (1984) (holding that the monitoring of a beeper located in a can inside of a house was a search).

Note that, in the student-only results, three of the outlier cases involved the Court finding that Fourth Amendment searches had occurred but then declaring such searches reasonable without any suspicion, a decision functionally similar to a finding of no search. See *Skinner*, 489 U.S. at 625 (holding that blood tests administered to railroad employees could be conducted without suspicion); *id.* (holding similarly for breathalyzer tests); *Class*, 475 U.S. at 116 (ruling that a police officer’s brief intrusion into a car in order to move some papers that were obscuring its VIN could be conducted without suspicion). Removing these and other “special needs” decisions from the data set would mean that the model correlated with 43 of 45 decisions (96%) in the four-coder results; 42 of 46 decisions (91%) in the student-only results; and 42 of 46 decisions (91%) in the author-only results. Under all of these scenarios, the model’s correlations with case outcomes were statistically significant at the .001 level.

lance at issue in each decision.¹⁹⁰ These principles were evaluated on an ordinal, seven-point scale. For example, the amount was measured from one (very low amount of information sought) to seven (very high amount of information sought), with four as a neutral midpoint. The average ratings assigned for each principle in all 50 decisions are reported in Table 1 of the Appendix.¹⁹¹ The implications of this assessment are discussed below.

Inter-coder agreement was substantial, although there were significant disagreements among coders in a few cases.¹⁹² These disagreements may parallel disputes among the Supreme Court's Justices in Fourth Amendment cases.¹⁹³

The numbers assigned necessarily represent a qualitative judgment, and further refinements of the measurements are welcome. Indeed, a central goal of this Article is to encourage additional research and consideration of the intimacy, amount, and cost associated with government surveillance. Reasonable people may disagree about the

¹⁹⁰ The coders read the majority and concurring opinions in each decision. These ratings necessarily take into account the Supreme Court's characterizations of the intimacy, amount, and/or cost at issue in these opinions, when available. The Supreme Court's characterizations, however, were not determinative and coders were instructed not to defer to the Court's assessments.

¹⁹¹ Average ratings are reported in increments of .50. Increments of .25 or below and .75 or above were rounded to the nearest whole number. Using median numbers instead of averages produced similar results.

¹⁹² Overall, measures of inter-coder agreement suggest substantial agreement among coders, particularly on ratings assigned to amount and cost. Krippendorff's alpha is a standard score used for calculating inter-coder agreement between more than two coders. See Matthew Lombard et al., *Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Research Projects* (June 1, 2010), <http://matthewlombard.com/reliability> [https://perma.cc/2BG2-Y3VA]. Krippendorff's alpha scores for the four coders were .657 for intimacy, .730 for amount, and .710 for cost. Scores over .600 generally indicate substantial agreement, scores over .667 indicate high levels of agreement, and scores over .800 suggest very high levels of agreement. See KIMBERLY A. NEUENDORF, *THE CONTENT ANALYSIS GUIDEBOOK* 168 (2d ed. 2017) (citing KLAUS KRIPPENDORFF, *CONTENT ANALYSIS* 325 (3d ed. 2013)). See generally J. Richard Landis & Gary G. Koch, *The Measurement of Observer Agreement for Categorical Data*, 33 *BIO-METRICS* 159 (1977) (characterizing agreement coefficients of over .61 as indicating substantial agreement). The tendency of Supreme Court Fourth Amendment cases to be non-unanimous, and the differences among coders in this project, suggest that different decisionmakers will bring varying perspectives to the assessment of Fourth Amendment search cases. This, in turn, highlights the importance of using multiple coders and aggregate scores. See *supra* note 189. Krippendorff's alpha scores were calculated using the ReCal tool for ordinal data at <http://dfreelon.org/utls/recalfront/recal-oir> [https://perma.cc/2BG2-Y3VA].

¹⁹³ See, e.g., *Kyllo v. United States*, 533 U.S. 27, 50 (2001) (Breyer, J., dissenting) (disagreeing with the majority that infrared cameras were capable of revealing intimate details regarding the home); *Arizona v. Hicks*, 480 U.S. 321, 338 (1987) (O'Connor, J., dissenting) (disagreeing with the majority regarding whether the cursory inspection of the underside of stereo equipment implicated Fourth Amendment interests sufficiently to require probable cause).

magnitude of the principles in a given case, just as the Justices themselves often do.¹⁹⁴ The Court's consideration of these principles is intuitive, not mathematical, and the aim of the consensus ratings assigned here is to reflect the intuitive guidance given by each principle.

1. *Standard Cases*

This Article's analysis of every Supreme Court test to apply the *Katz* test, although necessarily qualitative, helps to illuminate the role that the intimacy, amount, and cost model plays in determining the Fourth Amendment's scope. Beginning with the easiest cases, there were seven decisions in which all three principles pointed in the same direction.¹⁹⁵ All seven were resolved in accordance with the model. These cases often involved the collection of a small amount of non-intimate information at a substantial cost of time and effort to the police. In *United States v. Knotts*,¹⁹⁶ for example, state narcotics investigators installed a radio beeper device in a five gallon drum of chloroform, arranged with a chemical company to sell it to a suspect, and used the beeper to help them tail the suspect's car to a cabin located roughly an hour and a half's drive away.¹⁹⁷ The information regarding the suspect's location on public roads was not intimate, the amount of information gathered about his location was relatively low, and the cost of arranging for the beeper's sale and of tailing the suspect with several officers was substantial.¹⁹⁸ The Court held that the tracking of the beeper was not a search, expressly noting that the surveillance was limited to "public streets and highways"¹⁹⁹ and that the amount of information gathered was relatively low and did not constitute "dragnet-type law enforcement."²⁰⁰

¹⁹⁴ See *supra* note 193.

¹⁹⁵ *United States v. Jones*, 565 U.S. 400 (2012); *California v. Ciraolo*, 476 U.S. 207 (1986); *Illinois v. Andreas*, 463 U.S. 765 (1983); *United States v. Knotts*, 460 U.S. 276 (1983); see *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (holding that an order that obtained 152 days of cell phone location information was a search); *Carpenter*, 138 S. Ct. at 2217, 2220 & n.3 (holding that an order that obtained seven days of cell phone location information was a search); *Oliver v. United States*, 466 U.S. 170, 183 (1984) (holding that police officers walking around a locked gate and eventually onto a suspect's fields was a not a search).

¹⁹⁶ 466 U.S. 170 (1984).

¹⁹⁷ *Id.* at 278.

¹⁹⁸ See *id.* (describing the use of a helicopter in addition to vehicle pursuit of the suspect).

¹⁹⁹ *Id.* at 281.

²⁰⁰ *Id.* at 284.

In *Oliver v. United States*,²⁰¹ the Court had to determine whether the “open fields” doctrine, which provided that government officers may enter a citizen’s fields without a warrant, was justified under *Katz*’s reasonable expectation of privacy test.²⁰² In a drug investigation, police officers had driven to Oliver’s house, walked around a locked gate and along a road for several hundred yards, and eventually entered Oliver’s farmland, observing a field of marijuana situated over a mile from Oliver’s home.²⁰³ The area targeted by the search “[did] not provide the setting for those intimate activities” that the Fourth Amendment protects,²⁰⁴ the amount of information gathered was somewhat low, and the cost of gathering the information in terms of police time and effort was relatively high.²⁰⁵ Consistent with the intimacy, amount, and cost model, the Court held that this investigation did not violate Oliver’s reasonable expectation of privacy.²⁰⁶

There were 34 decisions where two principles pointed in the same direction while the other pointed in the opposite direction or was essentially neutral.²⁰⁷ In addition, there were two cases where two of the

201 466 U.S. 170 (1984).

202 *See id.* at 173.

203 *See id.*

204 *Id.* at 179.

205 *See id.* at 173–75.

206 *Id.* at 181.

207 *See* *Minnesota v. Carter*, 525 U.S. 83 (1998); *Minnesota v. Dickerson*, 508 U.S. 366 (1993); *Florida v. Riley*, 488 U.S. 445 (1989); *O’Connor v. Ortega*, 480 U.S. 709 (1987) (plurality opinion); *United States v. Dunn*, 480 U.S. 294 (1987); *Arizona v. Hicks*, 480 U.S. 321 (1987); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986); *Maryland v. Macon*, 472 U.S. 463 (1985); *Michigan v. Clifford*, 464 U.S. 287 (1984); *United States v. Place*, 462 U.S. 696 (1983); *Texas v. Brown*, 460 U.S. 730 (1983); *Rawlings v. Kentucky*, 448 U.S. 98 (1980); *United States v. Payner*, 447 U.S. 727 (1980); *Walter v. United States*, 447 U.S. 649 (1980); *Smith v. Maryland*, 442 U.S. 735 (1979); *Rakas v. Illinois*, 439 U.S. 128 (1978); *United States v. Dionisio*, 410 U.S. 1 (1973); *United States v. White*, 401 U.S. 745 (1971); *Mancusi v. DeForte*, 392 U.S. 364 (1968); *Terry v. Ohio*, 392 U.S. 1 (1968); *see also* *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 617 (1989) (holding that the taking of urine samples following specified events or suspicious behavior by railway employees would be a Fourth Amendment search); *Skinner*, 489 U.S. at 616–17 (holding that the administration of a breathalyzer test following specified events or suspicious behavior by railway employees would be a search); *New York v. Class*, 475 U.S. 106, 114 (1986) (holding that the visual observation of a car’s VIN was not a search); *United States v. Karo*, 468 U.S. 705, 712 (1984) (holding that the placement of a tracking beeper in a can that was later sold to Karo was not a search); *Karo*, 468 U.S. at 715 (holding that monitoring the beeper while the can was inside of a house was a search); *Karo*, 468 U.S. at 720 (holding that monitoring the beeper while the can was inside of a warehouse was not a search); *Karo*, 468 U.S. at 721 (holding that monitoring the beeper while it was on a truck traveling the public highways was not a search); *Oliver*, 466 U.S. at 183 (holding that police officers walking on a path through woods adjacent to a suspect’s property and eventually reaching small fields of marijuana plants on the suspect’s property was not a search); *United States v. Jacobsen*, 466 U.S. 109, 120 (1984) (holding

principles were essentially neutral while the other indicated a certain outcome.²⁰⁸ Thirty-three of these thirty-six decisions were resolved in accordance with the practical guidelines described in Section II.D. In other words, the Court typically resolved these cases in the direction dictated by the majority of the principles.²⁰⁹

For instance, in *Terry v. Ohio*,²¹⁰ a police officer lawfully seized three suspects and then patted down their outer clothing, finding guns on two of them.²¹¹ Although the amount of information obtained was low, so was the cost of the pat down in terms of time and effort. As for intimacy, the Court noted the intimacy of touching a person's body, concluding that the physical "exploration of . . . a person's clothing all over his or her body in an attempt to find weapons" was a "serious intrusion upon the sanctity of the person."²¹² The majority of the principles indicated that a reasonable expectation of privacy had been violated, and the Court held that the pat down was a search.²¹³ In *United States v. Place*,²¹⁴ the Court ruled that, while the seizure of Place and his bags was excessive, he was not searched under the Fourth Amendment when trained dogs sniffed around his bags for the smell of drugs.²¹⁵ While the dog sniff procedure in *Place* was likely moderate in cost, the sniff occurred in a public area and "disclose[d] only the presence or absence of narcotics" and was therefore "limited" both in intimacy and amount.²¹⁶ Accordingly, it did not violate Place's reasonable

that DEA agents removing baggies of white powder from a damaged package was not a search); *Jacobsen*, 466 U.S. at 124 (holding that testing the white powder for cocaine was not a search).

²⁰⁸ *Byrd v. United States*, 138 S. Ct. 1518 (2018); *California v. Greenwood*, 486 U.S. 35 (1988). In addition, *United States v. Miller*, 425 U.S. 435 (1976), received neutral ratings across the board. See *infra* app. tbl.1. In *Miller*, the Court held that obtaining an individual's bank records via subpoena was not a Fourth Amendment search. 425 U.S. at 442–43. The Court's holding might be explained by its fidelity to precedents holding that information exposed to third party informants was not protected by the Fourth Amendment. See *infra* note 232 and accompanying text. It is also possible that the Justices perceived the intimacy of the records at issue to be lower than did the coders in this study. See *Miller*, 425 U.S. at 442 (discussing the non-private nature of the documents at issue and noting that "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions").

²⁰⁹ See *infra* app. tbl.1. The outliers, *Skinner*, 489 U.S. at 616–17; *Hicks*, 480 U.S. at 324–25; and *White*, 401 U.S. at 752–53, are discussed in Section III.A.2.

²¹⁰ 392 U.S. 1 (1968).

²¹¹ *Id.* at 7.

²¹² *Id.* at 16–17.

²¹³ *Id.* at 16.

²¹⁴ 462 U.S. 696 (1983).

²¹⁵ *Id.* at 707.

²¹⁶ *Id.* The cost might be considered high if the entirety of the DEA's activity were counted. The agents did travel from LaGuardia airport to Kennedy airport with Place's bags in order to expose them to a trained drug-sniffing dog. But the taking and transportation of Place's

expectations of privacy, even though it revealed information about the inside of his luggage.²¹⁷

The intimacy, amount, and cost model can also help to explain some of the Supreme Court's most controversial or confusing Fourth Amendment scope cases. Many of the Court's decisions make little sense as assessments of actual societal expectations, and the Court sometimes holds that no search has occurred even when the police clearly breach societal norms of privacy. In *Florida v. Riley*,²¹⁸ for instance, the Court held that the observation of Riley's yard and greenhouse from a helicopter circling 400 feet overhead was not a Fourth Amendment search.²¹⁹ It is unlikely that citizens expect that their curtilage will be monitored by a low-flying helicopter.²²⁰ *Riley* instead reflects the Court's intuitive assessment of the invasiveness and legitimacy of the surveillance at issue. Riley's greenhouse and yard were moderately intimate areas, although the Court took pains to note that no intimate details were actually observed by law enforcement officers.²²¹ In any event, the officers only briefly observed Riley's yard, and did so at the substantial cost of operating a helicopter.²²² The amount and cost of the investigation indicated that it did

bags did not itself collect any information and might be better categorized as part of the seizure that preceded the dog-sniff search. Certainly, the Court categorized it this way. *See id.* at 709. In any event, if the cost of the search was high, the case would be even more straightforward under the model, with all three principles pointing towards a finding of no search.

²¹⁷ *See id.*; *see also, e.g., Dow Chemical Co. v. United States*, 476 U.S. 227, 229, 239 (1986) (holding that the EPA did not commit a Fourth Amendment search when it chartered a commercial photographer to take aerial photographs of a factory from over 1,200 feet overhead); *Texas v. Brown*, 460 U.S. 730, 733, 744 (1983) (holding that a police officer shining his flashlight into a car after lawfully pulling it over was not a search).

²¹⁸ 488 U.S. 445 (1989).

²¹⁹ *See id.* at 450–51.

²²⁰ *See id.* at 457 (Brennan, J., dissenting) (challenging the majority's argument that sights are "knowingly expose[d]" when they are viewable by helicopter); *see also California v. Ciraolo*, 476 U.S. 207, 223–24 (1986) (Powell, J., dissenting) (arguing that citizens reasonably expect privacy against overflight observation, the risk of which is so trivial as to be "virtually nonexistent").

²²¹ *See Riley*, 488 U.S. at 452.

²²² The helicopter was operated by the Pasco County Sheriff's Office and flown by a pilot employed by that office, and it circled the property twice before departing. *Id.* at 448; Petitioner's Brief on the Merits at 6, *Florida v. Riley*, 488 U.S. 445 (1989) (No. 87-764), 1987 WL 880076.

not raise sufficient concerns as to be a search,²²³ and the Court so held.²²⁴

2. Outliers

Although the intimacy, amount, and cost of surveillance strongly correlate with Supreme Court case outcomes, these are not the only considerations that can impact the Court's decisions. In particular, precedents set before *Katz* may continue to influence the Court's reasonable expectations of privacy jurisprudence.²²⁵ The three outlier decisions in which the Court did not follow the guidelines set out above may, in part, reflect the role of pre-*Katz* precedent in driving Supreme Court outcomes.

In *United States v. White*,²²⁶ government agents overheard conversations between White and an informant.²²⁷ The conversations took place in the informant's home and car, in a restaurant, and once in White's home.²²⁸ Generally, the informant wore a wire while one agent was hiding nearby and a second agent listened to the conversation using a radio receiver.²²⁹ Using this method, the agents were able to capture a significant amount of fairly intimate information, i.e., White's personal conversations.²³⁰ In a fractured plurality decision, the Court nonetheless held that this did not constitute a Fourth Amendment search.²³¹

The plurality was likely influenced by the long line of pre-*Katz* cases holding that the warrantless use of undercover agents or government informants did not violate the Fourth Amendment.²³² The Court explicitly invoked these cases throughout its opinion, noted that nothing in *Katz* directly overturned these cases, and concluded that it

²²³ Note that this analysis can do more than just help to clarify a difficult, poorly explained Fourth Amendment case. It also gives rise to a prediction regarding the long-term overhead monitoring of a backyard by automated drones: Such monitoring would involve the gathering of large amounts of information at a relatively low cost, and the Supreme Court would likely hold it to be a search. See *infra* Section IV.D.1.

²²⁴ See *Riley*, 488 U.S. at 452.

²²⁵ See *infra* text accompanying notes 232, 243.

²²⁶ 401 U.S. 745 (1971) (plurality opinion).

²²⁷ *Id.* at 746–47.

²²⁸ *Id.*

²²⁹ *Id.* The agents and informant also recorded White using radio equipment in the informant's car, in White's home, and in a restaurant. *Id.*

²³⁰ See *id.*

²³¹ Justice Black concurred in the judgment of the Court on the basis of his opposition to *Katz* itself. *Id.* at 754 (Black, J., concurring).

²³² See, e.g., *Hoffa v. United States*, 385 U.S. 293, 302–03 (1966); *On Lee v. United States*, 343 U.S. 747, 754 (1952).

ought not reverse this longstanding doctrine.²³³ It is also notable that the deciding vote on the issue was cast by Justice Black, who opposed the *Katz* test and refused to apply it at all.²³⁴

The Court's ruling might also have been influenced by the especially high cost of the surveillance at issue—a cost so high as to possibly outweigh the two factors cutting in the other direction.²³⁵ In general, the use of informants requires significant investments of police time and effort, and undercover agents require even greater investments and risks.²³⁶ Holding all else equal, the substantial cost of these procedures deters police abuses and arbitrary violations of citizens' privacy.²³⁷ At the least, the substantial cost of the surveillance in *White* may have helped convince a slim majority of Justices to avoid overruling a long line of established precedents.

In *Skinner v. Railway Labor Executives' Ass'n*,²³⁸ the Court held, among other things, that breathalyzer tests administered to railroad employees were Fourth Amendment searches.²³⁹ This result contradicts the predictions of the intimacy, amount, and cost model, as breathalyzers capture only a small amount of information and are not especially intimate.²⁴⁰ This might be explained by the fact that *Skinner* was a “special needs” case,²⁴¹ in which despite finding a Fourth Amendment search the Court ultimately held that the government could use breathalyzer tests on railroad employees without either a

²³³ *White*, 401 U.S. at 750.

²³⁴ Compare *id.* at 754 (Black, J., concurring) (reaffirming his disagreement with *Katz*), with *id.* at 755 (Brennan, J., concurring) (arguing that the undercover agent precedents should be overturned but voting in favor of the government on the ground that *Katz* was not retroactive). Among the eight Justices who applied or would have applied the reasonable expectation of privacy test, the votes were split four to four.

²³⁵ See *id.* at 746–47 (majority opinion) (describing the elaborate recording scheme, which included an undercover informant, one agent hiding in a kitchen closet, and another outside the house using a radio receiver).

²³⁶ See William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1277 (1999).

²³⁷ See *id.* This is not to say that informants and undercover agents have not been used in an arbitrary and abusive manner, especially by federal spy agencies with larger budgets whose expenditures are generally shielded from public scrutiny. See, e.g., CURT GENTRY, J. EDGAR HOOVER 100–01 (1991).

²³⁸ 489 U.S. 602 (1989).

²³⁹ *Id.* at 616.

²⁴⁰ See *id.* at 625 (characterizing the intrusiveness of breathalyzer tests as low). But see *id.* at 616–17 (noting that such tests raise “concerns about bodily integrity”).

²⁴¹ For a discussion of the “special needs” concept, see generally Kenneth Nuer, *The Special Needs Rationale: Creating a Chasm in Fourth Amendment Analysis*, 32 SANTA CLARA L. REV. 89 (1992).

warrant or any particularized suspicion of intoxication.²⁴² Thus the finding of a search had no impact on the ultimate outcome; the ruling would have been the same had the Court found no search at all.

The Court was also likely influenced by earlier precedents involving blood and urine tests. The Court cursorily analogized breathalyzer tests to blood tests, which had been deemed Fourth Amendment searches in a line of precedents stretching back before *Katz*.²⁴³ The influence of precedent, coupled with the practical irrelevance of the search issue in *Skinner*, likely drove this ruling.

Finally, in *Arizona v. Hicks*,²⁴⁴ the Court held that police officers who lawfully entered an apartment to investigate a gunshot committed an additional search when they picked up some stereo components in order to observe their serial numbers.²⁴⁵ This outcome is somewhat unusual, given that the movement of stereo components gathers little information and is not a particularly intimate form of surveillance.

One potential explanation for this result is that the Court considered even the movement of a turntable or a speaker inside of a home to implicate intimate information. The Court alluded to this when it expressed concern that “letters or photographs” might have been “hidden behind or under the equipment.”²⁴⁶ *Hicks* may also be a reflection of the Court’s absolutism about protecting information inside of the home, no matter how trivial. It is also worth noting that *Hicks* was not a typical *Katz*-test case. Justice Scalia did not cite *Katz* anywhere in his opinion for the Court. Indeed, although the opinion briefly alluded to an “invasion of respondent’s privacy,”²⁴⁷ *Hicks* may be a precursor to Justice Scalia’s later opinions holding that any physical touching of property for informational purposes is a Fourth Amendment search.²⁴⁸ It also echoes several pre-*Katz* cases that turned on physical contact with a suspect’s property.²⁴⁹ *Hicks* may

²⁴² *Skinner*, 489 U.S. at 633–34. The statutory authorization for breath tests contemplated their use when an employee was involved with an accident or safety incident, or when the employee failed to comply with signal or speed regulations. *See id.* at 611 (citing 49 C.F.R. § 219.301(b)). The Court expressly rejected the need for particularized suspicion in the administration of these tests. *See id.* at 630–31.

²⁴³ *See, e.g., id.* at 616–17; *Schmerber v. California*, 384 U.S. 757, 767–68 (1966).

²⁴⁴ 480 U.S. 321 (1987).

²⁴⁵ *Id.* at 325–30.

²⁴⁶ *Id.* at 325.

²⁴⁷ *Id.*

²⁴⁸ *See Florida v. Jardines*, 569 U.S. 1, 5 (2013); *United States v. Jones*, 565 U.S. 400, 404–05 (2012).

²⁴⁹ *See, e.g., Silverman v. United States*, 365 U.S. 505, 509 (1961) (holding that the police

have been an early step in Justice Scalia's project of reviving a property-based approach to the Fourth Amendment, operating alongside the *Katz* test.²⁵⁰

B. Weighting the Principles and Resolving Close Cases

This Section examines cases in which the principles-based model does not clearly point in one direction or another. These cases require an evaluation of the relative importance of the various principles. In mathematical terms, they require weighting the variables of intimacy, amount, and cost in order to determine outcomes in especially close cases.

Such cases can arise when two of the principles point in opposite directions while the third is essentially neutral or indeterminate. There were six such cases among the Supreme Court's decisions applying the *Katz* test. By assessing these cases and their outcomes, it is possible to develop a theory about the approximate weight that the Supreme Court gives to each principle in reasonable expectations of privacy cases. As mentioned above, intimacy appears to be the most influential principle, followed by cost, and then amount.²⁵¹ Thus, when intimacy conflicts with another principle, intimacy typically prevails. When intimacy is neither notably high nor low, then the cost of the surveillance at issue will more likely than not determine the outcome of the case.

In five of these close cases, intimacy conflicted with some other principle, while the third principle was essentially neutral.²⁵² In all five cases, intimacy appeared to determine the ultimate case outcome. For

violated the Fourth Amendment when their recording device touched the heating duct of a suspect's house); *Goldman v. United States*, 316 U.S. 129, 135 (1942) (holding that federal agents did not violate the Fourth Amendment when they used a microphone that did not touch a suspect's property).

²⁵⁰ See *Jones*, 565 U.S. at 407–08. The reestablishment of a property-based rule in cases involving physical intrusions by the police likely means that the intimacy, amount, and cost model will play an even clearer role in *Katz* cases going forward. *E.g.*, *Jardines*, 569 U.S. 1; see *supra* note 1. The older concepts of physical trespass that may have driven the result in *Hicks* are now embodied by a separate test. These trespass concepts are less likely than ever to influence the Court's analysis of reasonable expectations of privacy. In general, as time passes and older precedents fade or branch off into separate tests, intimacy, amount, and cost will play an even more dominant role in determining reasonable expectations of privacy.

²⁵¹ See *supra* Section II.D.

²⁵² See *infra* app. tbl.1; see also *Kyllo v. United States*, 533 U.S. 27, 29–30, 34, 37–38 (2001); *Minnesota v. Olson*, 495 U.S. 91, 94 (1990); *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 609–10, 616–17 (1989) (holding that a blood test was a Fourth Amendment search); *Hudson v. Palmer*, 468 U.S. 517, 519–20 (1984); *Katz v. United States*, 389 U.S. 347, 348, 352, 354 (1967).

example, in *Minnesota v. Olson*,²⁵³ the police warrantlessly entered a house in which Olson was a houseguest, found Olson hiding in a closet, and arrested him.²⁵⁴ The cost of this relatively brief, in-person investigation was moderate.²⁵⁵ While the amount of information gathered by this procedure was relatively low, even a quick intrusion into a home in which a person is staying as an overnight guest is fairly intimate.²⁵⁶ Emphasizing the inherently “private” and “vulnerable” nature of staying in another person’s house and the host’s willingness “to share his house and his privacy with his guest,” the Court ruled that Olson had a reasonable expectation of privacy in the house.²⁵⁷ The relatively high intimacy of the place searched was determinative.

There was only one case in in which intimacy was moderate and the other two principles conflicted. In *New York v. Class*,²⁵⁸ police officers lawfully stopped Class’s car, which had a cracked windshield.²⁵⁹ One of the officers opened the car door, reached into the interior of the car, and moved some papers obscuring the VIN number area on the car’s dashboard.²⁶⁰ The limited physical intrusion into the car was moderate in terms of intimacy.²⁶¹ The cost to the officer of reaching into the car was low, while the amount of information obtained during the initial intrusion was likewise low. Any conclusion drawn from a single case is necessarily tentative. But it appears that, when moderately intimate information is obtained at a low cost, that is sufficient to raise concerns about privacy even when relatively little information is gathered.

In any event, the tendencies described in this Section are not bright-line rules of Supreme Court behavior. Although the Court may favor intimacy, followed by cost, when two principles conflict, future cases might arise where this general rule of thumb is not followed. There may also be future cases where the magnitude of one principle is so high or low that it will determine outcomes despite the other two

²⁵³ 495 U.S. 91 (1990).

²⁵⁴ *Id.* at 94.

²⁵⁵ *See infra* app. tbl.1.

²⁵⁶ *See id.*; *Olson*, 495 U.S. at 94.

²⁵⁷ *Id.* at 99.

²⁵⁸ 475 U.S. 106 (1986).

²⁵⁹ *Id.* at 107–08.

²⁶⁰ *Id.* at 108. In doing so, the officer saw the handle of a gun under the driver’s seat, and he then seized the gun and arrested the driver. *Id.*

²⁶¹ *See id.* at 112–13 (noting that the Fourth Amendment generally protects automobiles but that expectations of privacy in cars are reduced in part because cars are subject to visual scrutiny and exposure); *infra* app. tbl.1.

principles.²⁶² For example, if the Court heard a case involving a CCTV camera mounted above a public intersection, the exceptionally low intimacy of the data captured might outweigh even the substantial amount and the low cost of data collection.²⁶³ By contrast, long-term video surveillance of a somewhat more intimate place, such as a front yard, would likely be a search.²⁶⁴

Detailed analysis of the three principles, their directions, and their magnitudes can help legal actors address even the most complex Fourth Amendment issues. Meanwhile, the practical guidelines described above can account for the vast majority of the Supreme Court's reasonable expectation of privacy cases.

IV. ASSESSING THE PRINCIPLES-BASED APPROACH

The preceding Sections posit that the Supreme Court's Fourth Amendment scope decisions are guided by an intuitive assessment of the principles of intimacy, amount, and cost. This claim is descriptive and concerns the Court's actual practice. It is not a claim that the Court's current approach is optimal or normatively desirable.²⁶⁵

This Part assesses the principles-based model of Fourth Amendment privacy. It describes the advantages and disadvantages of the Court's largely intuitive, case-by-case approach. It then makes the affirmative case for a more widespread recognition of the principles. It concludes by applying the intimacy, amount, and cost model to several

²⁶² See *infra* app. tbl.1 (describing the ratings assigned to *United States v. White*, 401 U.S. 745 (1971), which may be an example of such a case).

²⁶³ Cf. *United States v. Wymer*, 40 F. Supp. 3d 933, 939 (N.D. Ohio 2014) (holding that video surveillance of publicly exposed commercial property was not a search). Alternatively, the Court might declare the mounting of a permanent camera in a high-crime area to be a search, but a search that is reasonable under the circumstances even without particularized suspicion or a warrant. Cf. *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 455 (1990) (holding that a highway sobriety checkpoint was a Fourth Amendment seizure of motorists but that the seizure was reasonable in light of the state's interest in combating drunk driving and therefore did not require a warrant).

²⁶⁴ The lower courts are currently split on this issue, although the split is lopsided, and the federal courts of appeals have uniformly held that camera observation of a home visible from public roads is not a search. Compare *United States v. Vargas*, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *27 (E.D. Wash. Dec. 15, 2014) (suppressing evidence from a telephone pole camera used to record the outside of an individual's home for six weeks), and *South Dakota v. Jones*, 903 N.W.2d 101, 113 (S.D. 2017) (holding that long-term video monitoring of the area around a mobile home was a search), with *United States v. Cantu*, 684 F. App'x 703, 705 (10th Cir. 2017) (holding that video surveillance of the outside of a house was not a search), *United States v. Bucci*, 582 F.3d 108, 116 (1st Cir. 2009) (same), and *United States v. Gilliam*, Nos. 02:12-CR-93; 02:13-CR-235, 2015 WL 5178197, at *9 (W.D. Pa. Sept. 4, 2015) (same).

²⁶⁵ Many scholars have argued in favor of alternative approaches to determining the scope of the Fourth Amendment. See *supra* note 77 and accompanying text.

novel surveillance questions likely to arise in future Supreme Court cases.

A. *Advantages*

The intimacy, amount, and cost approach to the Fourth Amendment's scope has many benefits. The intimacy and amount of data sought are, especially when combined, effective proxies for the various privacy harms associated with government surveillance.²⁶⁶ In general, the more information that the government collects about an individual and the more intimate that information, the greater the likelihood that the individual will suffer harms like the deterrence of lawful activities, interference with relationships, unauthorized information disclosure, risk of exposure and abuse, and psychological harms related to intrusion on private spaces.²⁶⁷ The severity of such harms is also likely to increase with more intimate or voluminous data.²⁶⁸ In addition, cost is a relatively effective proxy for the arbitrariness of an act of surveillance and its potential for abuse.²⁶⁹ The lower the cost of a surveillance practice, the more likely it is to be used broadly against innocent persons and the less visible it is to supervisors, regulatory entities, or political actors.²⁷⁰

By combining these three principles, the Court is able to roughly estimate the severity of the privacy harm caused by the government and the likelihood of indiscriminate or abusive practices. This approximation allows the Court to determine when an act of surveillance raises sufficient concerns as to require constitutional regulation. It also avoids a more detailed analysis of privacy impacts or law enforcement benefits, reducing the normative precision of the test compared to some potential alternatives but enhancing predictability and keeping decision costs low.²⁷¹

The test also avoids some of the problems that would arise from applying the literal *Katz* test and basing the Fourth Amendment's scope on what people actually expect regarding their privacy. As the

²⁶⁶ See *supra* text accompanying notes 84–90. See generally Matthew Tokson, *Blank Slates*, 59 B.C. L. REV. 591, 609 (2018) (discussing the use of proxy values in law).

²⁶⁷ See Tokson, *supra* note 77 at 758, 762, 765–67; see also Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 527–36, 539–42 (2006).

²⁶⁸ See Solove, *supra* note 267, at 505–15 (discussing privacy harms that arise from data aggregation and from personally identifiable information).

²⁶⁹ See *supra* text accompanying notes 136–43.

²⁷⁰ See *supra* text accompanying notes 136–43.

²⁷¹ Cf. Tokson, *supra* note 77 (proposing a normative balancing test for the Fourth Amendment's scope).

Supreme Court itself has recognized on several occasions, the *Katz* test as written would enable the government to subvert the Fourth Amendment by manipulating societal expectations.²⁷² Moreover, societal knowledge about privacy threats is both hard to measure and vulnerable to rapid changes, making accurate assessments of societal expectations difficult in many cases.²⁷³ The intuitive assessment of intimacy, amount, and cost is more workable and more likely to capture the relevant privacy harms associated with surveillance.

B. Drawbacks

In addition to its substantial advantages, the Supreme Court's intuitive assessment of intimacy, amount, and cost in government surveillance cases has several drawbacks. Indeed, it is far from clear that the principles-based approach is the optimal regime for determining Fourth Amendment searches.²⁷⁴

One disadvantage of the Court's current approach is simply that the Justices assess these principles intuitively and non-rigorously. Even when the Court explicitly addresses one or more of the principles in its opinion, its assessments are rarely detailed or precise. Intimacy in particular is a somewhat abstract notion that is difficult to assess precisely, and critics have plausibly taken issue with the Court's assessments of intimacy in cases involving dialed phone numbers, household trash, bank records, stereo equipment, and more.²⁷⁵ The depth and rigor of the Court's analysis is less than it might be under a more specific calculus, such as one involving a detailed normative balancing²⁷⁶ or an assessment of applicable positive law or property concepts.²⁷⁷

Another issue arises because the cost of a surveillance technique or the intimacy or amount of data it gathers can change substantially over time. For instance, in 1979, the government collected only a few

²⁷² *Hudson v. Palmer*, 468 U.S. 517, 525 n.7 (1984); *Smith v. Maryland*, 442 U.S. 735, 740–41 & n.5 (1979).

²⁷³ See Tokson, *supra* note 71, at 164–73.

²⁷⁴ See *supra* notes 45–79 and accompanying text.

²⁷⁵ See Colb, *supra* note 11, at 127–29, 156–59; Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 829 (2005); Tokson, *supra* note 77 at 806–08; see also *Kyllo v. United States*, 533 U.S. 27, 41–51 (2001) (Stevens, J., dissenting); *Arizona v. Hicks*, 480 U.S. 321, 331 (1987) (Powell, J., dissenting).

²⁷⁶ Tokson, *supra* note 77 at 752–53.

²⁷⁷ See, e.g., Baude & Stern, *supra* note 45, at 1825; Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 219 (2019); Laurent Sacharoff, *Constitutional Trespass*, 81 TENN. L. REV. 877, 910–11 (2014).

days' worth of Michael Lee Smith's dialed phone numbers.²⁷⁸ The Court held that this was not a search, emphasizing that the list of phone numbers was not nearly as intimate as the contents of Smith's actual conversations.²⁷⁹ Yet the government eventually became capable of collecting and storing vast quantities of dialed numbers at low cost, and capable of analyzing such data to reveal intimate details about an individual's social connections, activities, and even sexual preferences.²⁸⁰ Nonetheless, controlling precedent holds that phone number collection is not a search.²⁸¹ As technologies improve and social contexts change, the broadly applicable rules set by the Court in earlier cases may do an increasingly poor job of regulating modern surveillance.

In fairness, the Court has been willing in a few recent cases to assess surveillance technologies more broadly, examining not only the surveillance technology at issue but also the intimacy or amount of data that will likely be collected in future cases as the technology improves.²⁸² Greater recognition of the principles-based model would help to further mitigate the Court's difficulties with technological change. Parties could directly argue that a precedent should be distinguished or overturned because of substantial changes in the intimacy, amount, or cost implicated by a surveillance practice.²⁸³ Even then, however, the force of precedent and *stare decisis* may cause courts to under-adjust to changing circumstances.²⁸⁴

Another drawback of the Court's approach is related to the narrowness of its analysis. The "reasonable expectations of privacy" test and the principles that guide it focus almost exclusively on privacy to the exclusion of other values implicated by the Fourth Amendment. The intimacy, amount, and cost model largely ignores various harms associated with arbitrary government intrusion, including coercion, intimidation, and discrimination.²⁸⁵ For example, a surveillance program that targets "high-crime areas" in inner cities may collect only non-intimate data, but may impose harms by expressing societal condem-

²⁷⁸ *Smith v. Maryland*, 442 U.S. 735, 737 (1979).

²⁷⁹ *Id.* at 745–46.

²⁸⁰ *See supra* note 116.

²⁸¹ *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (declining to "extend" *Smith*).

²⁸² *See, e.g., id.* at 2218–19; *Kyllo v. United States*, 533 U.S. 27, 36 (2001).

²⁸³ *See infra* Section IV.C (discussing other benefits of greater recognition of the principles).

²⁸⁴ *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871 (2004) (contrasting the ability of legislatures and courts to define privacy rules in response to new technology).

²⁸⁵ *See* Stuntz, *supra* note 78, at 1065–66.

nation or distrust of the people surveilled.²⁸⁶ Discriminatory surveillance can cause substantial psychological and even physical harm to its targets.²⁸⁷ Other, broader regimes for determining the scope of the Fourth Amendment would likely do a better job of capturing non-privacy surveillance harms.²⁸⁸

An additional negative effect of an approach that treats low-cost surveillance as a factor that favors government regulation is that it discourages cost efficiency. Low-cost surveillance techniques may pose a greater risk to citizen privacy, but they also make law enforcement cheaper and more effective, potentially conferring substantial societal benefits.²⁸⁹ Although the use of cost as a proxy for legitimacy is sensible, alternative approaches to the Fourth Amendment's scope might take a more nuanced view of low-cost surveillance, considering its benefits as well as its costs.²⁹⁰ Of course, such an approach would be more difficult for judges to administer than simply using the cost of surveillance as a proxy for the likelihood of abuse.²⁹¹

Relatedly, the intimacy, amount, and cost model might be criticized for failing to take law enforcement benefit into account at all. Thus, the Court might sub-optimally require the police to obtain a warrant even in situations where society would be better off with no such requirement. Perhaps, for instance, non-coding DNA databases containing every citizen's DNA would deter huge numbers of serious crimes while imposing only minor privacy harms.²⁹² An optimal approach to the Fourth Amendment's scope might approve such surveillance by taking its benefits into account as well as its harms.²⁹³ Such an approach would, however, be more administratively complex than the

²⁸⁶ See Craig Konnoth, *An Expressive Theory of Privacy Intrusions*, 102 IOWA L. REV. 1533, 1563–68 (2017).

²⁸⁷ See Pamela J. Sawyer et al., *Discrimination and the Stress Response: Psychological and Physiological Consequences of Anticipating Prejudice in Interethnic Interactions*, 102 AM. J. PUB. HEALTH 1020 (2012); Abigail A. Sewell & Kevin A. Jefferson, *Collateral Damage: The Health Effects of Invasive Police Encounters in New York City*, 93 J. URB. HEALTH 542, 543 (2016).

²⁸⁸ See Tokson, *supra* note 77 at 752–53.

²⁸⁹ See Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 549, 573–76 (2013).

²⁹⁰ See *id.* at 578; Tokson, *supra* note 77 at 752, 780.

²⁹¹ See Simmons, *supra* note 289, at 582.

²⁹² I take no position on whether this is actually the case, although there is at least some reason to think that the deterrent effects of such databases are substantial. See generally Jennifer L. Doleac, *The Effects of DNA Databases on Crime*, 9 AM. ECON. J. 165 (2017) (showing the substantial deterrent effects of state DNA databases).

²⁹³ See Tokson, *supra* note 77; cf. Paul G. Cassell, *All Benefits, No Costs: The Grand Illusion of Miranda's Defenders*, 90 NW. U. L. REV. 1084 (1996) (critiquing the lack of cost-benefit analysis in Fifth Amendment jurisprudence).

intimacy, amount, and cost model. Further, the lack of balancing in the principles-based approach is mitigated in some cases by balancing at the “reasonableness” stage of the Fourth Amendment inquiry, where courts determine whether the Fourth Amendment search at issue was justified.²⁹⁴ This normally requires a warrant, but, in certain situations, the Court overtly balances the benefits and costs of government surveillance and permits various kinds of searches without a warrant or probable cause.²⁹⁵ In other cases, the Court performs a quasi-balancing by allowing limited searches or seizures based on reasonable suspicion alone.²⁹⁶ Still, the Court’s approach to the Fourth Amendment’s scope could be criticized as oversimplified, or for neglecting the substantial benefits of law enforcement in certain contexts.

C. *The Case for Greater Recognition of the Principles*

Greater recognition of the intimacy, amount, and cost model would have substantial benefits for courts and other legal actors. Currently, many lower courts address novel Fourth Amendment scope questions by attempting to apply the *Katz* test literally.²⁹⁷ They accordingly try to assess societal knowledge and expectations about new surveillance technologies, and often struggle to do so accurately.²⁹⁸ Although the intimacy, amount, and cost of an act of surveillance may be difficult to quantify precisely, these principles are more tractable and intuitive for lower court judges than the questions of society-wide knowledge, expectations, and norms that the literal *Katz* test requires.²⁹⁹

²⁹⁴ The Fourth Amendment prohibits only “unreasonable” searches and seizures. U.S. CONST. amend. IV.

²⁹⁵ See, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 664–65 (1995); *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 679 (1989); *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 633–34 (1989).

²⁹⁶ See *Terry v. Ohio*, 392 U.S. 1, 23–27 (1968) (a police officer needed only reasonable suspicion to search a suspect for weapons); *Alabama v. White*, 496 U.S. 325, 330–31 (1990) (police need only reasonable suspicion to pull over a car and question its driver).

²⁹⁷ See Tokson, *supra* note 71, at 154, 155–58, 161–63 (describing examples of lower courts futilely attempting to measure the extent of societal knowledge in order to determine societal expectations of privacy).

²⁹⁸ *Id.*

²⁹⁹ See *id.* at 149–51; Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 613–15 (2011). Survey evidence on nationwide expectations of privacy may be helpful to judges applying the literal *Katz* test, although such surveys will not always be available to lower court judges facing an issue of first impression. Nor would surveys of expectations about novel and largely unknown surveillance technologies be likely to produce meaningful or consistent results. See Daniel J. Solove, *Surveillance: Data Mining and the Security-Liberty Debate*, 75

Lower court judges are capable of overtly assessing the intimacy of the information sought, the amount of information collected, and the cost of an act of surveillance at issue, just as the Supreme Court has done in recent cases.³⁰⁰ If the Court expressly acknowledged the importance of these principles, lower courts could engage in this analysis directly in each Fourth Amendment scope case. This would, in turn, have two further beneficial effects on Fourth Amendment law. First, it would reorganize Fourth Amendment doctrine along a single, unified model, simplifying the law of searches and avoiding the vagueness and incoherence of current *Katz* jurisprudence.³⁰¹ Although disagreements about how to characterize the intimacy, amount, or cost of various surveillance practices would surely arise, the adoption of a common doctrinal model for reasonable expectations of privacy would lead to greater uniformity in lower court rulings. The present “constitutional cacophony” of lower court disagreement on Fourth Amendment issues might be reduced.³⁰²

Second, a detailed assessment of the principles by lower courts would likely improve the Supreme Court’s analysis. The Justices would have a complete account of the principles to review, as well as a thoroughly developed factual record relevant to the intimacy, amount, and cost of the surveillance. In cases where lower court judges disagree, the Justices could compare the majority and dissenting judges’ opinions and determine whose arguments were more persuasive. The process would be more comprehensive, more transparent, and involve a broader set of viewpoints than the Court’s current informal and intuitive process.

A single, comprehensible model of Fourth Amendment searches would also enhance the ability of law enforcement officials to deter-

U. CHI. L. REV. 343, 355 (2008) (describing two nationwide polls on government anti-terrorism surveillance and their limitations because of the phrasing of the questions and the knowledge of respondents). Moreover, the Supreme Court has explained that, for various reasons, the *Katz* test should not be considered a literal assessment of societal expectations, or at least not exclusively. See *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (stating that one’s literal expectation of privacy—such as for a “burglar plying his trade in a summer cabin during the off season”—is irrelevant to the court’s assessment of a reasonable and constitutionally “legitimate” expectation); *supra* note 35.

³⁰⁰ See *Carpenter v. United States*, 138 S. Ct. 2206, 2217–20 (2018); *United States v. Jones*, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring); *Jones*, 565 U.S. at 429–30 (Alito, J., concurring).

³⁰¹ See Kerr, *supra* note 2, at 506–07 (describing the incoherence of current doctrinal approaches).

³⁰² See Wayne A. Logan, *Constitutional Cacophony: Federal Circuit Splits and the Fourth Amendment*, 65 VAND. L. REV. 1137, 1195 (2012).

mine *ex ante* what they can and cannot surveil without a warrant. Indeed, greater recognition of the model may even help to limit the reach of qualified immunity in Fourth Amendment cases. If a surveillance technique is obviously a search given its intimacy, amount, and cost, then courts should be less willing to extend qualified immunity to officers who engage in it without a warrant.³⁰³

Finally, the principles-based model can improve the broader legal community's understanding of the *Katz* test. Many lawyers and law students find the test confusing, and many textbooks do not even attempt to explain it.³⁰⁴ Explaining the *Katz* test is difficult for many reasons: The test comes from a concurrence rather than the majority opinion; it cannot be taken literally; the Court often contradicts the test as stated; and there are several subdoctrines like the third-party doctrine that are counterintuitive and do not seem to follow the test. The principles-based model provides a comprehensive account of the Supreme Court's *Katz* test cases and offers a coherent answer to the question of what violates a reasonable expectation of privacy.

D. Resolving Future Cases

The intimacy, amount, and cost model is a descriptive account of how the Supreme Court resolves cases under the *Katz* test. The model can help predict how the Court will resolve future Fourth Amendment issues using that test. Of course, a future Court might someday adopt a new test, perhaps reinstating the trespass-based approach of *Olmstead v. United States*³⁰⁵ or forging a broad concept of property intrusions to serve as the lodestar of Fourth Amendment protection.³⁰⁶ In the meantime, *Carpenter* signals the current Court's willingness to apply the *Katz* test to novel surveillance contexts.³⁰⁷ This section discusses how the Court is likely to apply this test to advanced surveillance technologies already in use.

³⁰³ See generally Joanna C. Schwartz, *The Case Against Qualified Immunity*, 93 NOTRE DAME L. REV. 1797 (2018) (arguing that qualified immunity is pernicious and ultimately ineffective at shielding police officers from the burdens of litigation).

³⁰⁴ See *supra* notes 71–75 and accompanying text.

³⁰⁵ 277 U.S. 438 (1928); see *Carpenter v. United States*, 138 S. Ct. 2206, 2238 (2018) (Thomas, J., dissenting) (contending that the Fourth Amendment's protections should be limited to a defendant's person and tangible property).

³⁰⁶ Cf. *Carpenter*, 138 S. Ct. at 2269–72 (Gorsuch, J., dissenting) (suggesting that the Court should explore a broad theory of Fourth Amendment property interests). It is also possible that no five-Justice majority will agree on the proper test for Fourth Amendment searches, resulting in fractured opinions that incorporate *Katz* test analysis as well as other concepts.

³⁰⁷ *Id.* at 2213–14 (majority opinion); *id.* at 2227 (Kennedy, J., dissenting).

The Supreme Court's intimacy, amount, and cost inquiry is typically fact-specific. For better or worse, the outcome of a future Fourth Amendment case will depend on the particular government activities challenged in the case. However, for many next-generation surveillance technologies, it is easy to imagine the general fact patterns that the Court is likely to face. This Section addresses three such fact patterns and uses the intimacy, amount, and cost model to predict how the Supreme Court would likely rule in future cases.

1. Drones

Police departments and the federal government have begun to use unmanned drones for various law enforcement and public safety purposes, including criminal investigations.³⁰⁸ Drones can be mounted with high-resolution cameras, infrared scanners, radar, or other sensing devices.³⁰⁹ Several drone autopilot systems have been developed, and automated drone technologies have become increasingly available to consumers.³¹⁰ A drone model operated by hundreds of public agencies, for instance, features an autopilot mode called "point of interest" which allows the drone to continually circle around a specific building, object, or location while recording photos and video.³¹¹ Although

³⁰⁸ See, e.g., Hillary B. Farber, *Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment*, 64 SYRACUSE L. REV. 1, 2–3 (2014) (discussing drone purchases and FAA applications from police departments for drone use in law enforcement); Carmen Duarte, *Sahuarita Police Expect to Use Drones by December*, ARIZ. DAILY STAR (Nov. 3, 2016), https://tucson.com/news/local/crime/sahuarita-police-expect-to-use-drones-by-december/article_94a12d80-567f-523c-866f-87b7bc341cbd.html [<https://perma.cc/5PQG-SLLQ>] (discussing a local police department's pending use of drones for "daily investigations and other duties"); Conor Friedersdorf, *The Rapid Rise of Federal Surveillance Drones Over America*, ATLANTIC (Mar. 10, 2016), <https://www.theatlantic.com/politics/archive/2016/03/the-rapid-rise-of-federal-surveillance-drones-over-america/473136/> [<https://perma.cc/RB2S-XPL4>] (discussing the rapid increase in drone use by the FBI and several other federal government agencies); *More Police Departments and Other First-Responders Are Using Drones*, ECONOMIST (Oct. 12, 2017), <https://www.economist.com/united-states/2017/10/12/more-police-departments-and-other-first-responders-are-using-drones> [<https://perma.cc/8UEK-LRVB>] (noting the rapid increase in drone use among various local police and fire departments).

³⁰⁹ See, e.g., Brian Bennett, *Police Employ Predator Drone Spy Planes on Home Front*, L.A. TIMES (Dec. 10, 2011, 12:00 AM), <http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211> [<https://perma.cc/VHK3-X7XF>].

³¹⁰ See, e.g., Logan Campbell, *What Autopilot Should I Use for My Drone?*, AEROTAS (Apr. 18, 2016), <https://www.aerotas.com/blog/2016/4/14/what-autopilot-should-i-use-for-my-drone> [<https://perma.cc/Y9WZ-32YG>]; Klint Finley, *World's Smallest Drone Autopilot System Goes Open Source*, WIRED (Aug. 28, 2013, 9:30 AM), <https://www.wired.com/2013/08/drone-autopilot> [<https://perma.cc/2WBA-LJPB>].

³¹¹ See Stetson Doggett, *Film Smooth & Steady Drone Video Using DJI Point of Interest*, DRONEGENUITY, <https://www.dronegenuity.com/doing-more-with-point-of-interest/>; DAN GETTINGER, PUBLIC SAFETY DRONES 3 (2018), <https://dronecenter.bard.edu/files/2018/05/CSD-Pub>

most drone models currently available to consumers have limited flight times, their capabilities are improving.³¹² Many military-grade drones can fly continuously for several days.³¹³

The drone surveillance scenario most commonly envisioned by commentators is that of a drone conducting extended camera surveillance of the curtilage of a home.³¹⁴ Several authors have raised concerns that such monitoring would not be a search based on an analogy to the Court's cases finding that overflight surveillance from manned aircraft was not a Fourth Amendment search.³¹⁵

Suppose that the federal government used automated drones to continuously monitor the curtilage and exterior of a home for a period of 30 days.³¹⁶ How would the Court decide such a case? The intimacy, amount, and cost model all offer several insights. A drone case would be notably different with respect to the three principles than previous cases involving manned airplanes and helicopters.³¹⁷ To be sure, the intimacy of the information sought would be similar. The surveillance would involve the visual observation of an individual's yard and house from (let us assume) a lawful height for aircraft, and the intimacy of such observation would be relatively moderate.³¹⁸ But both the amount of data collected and the cost of the surveillance would be substantially different than in the manned overflight cases of *California v. Ciraolo*³¹⁹ and *Riley*.³²⁰ The amount of data gathered on the re-

lic-Safety-Drones-Update-1.pdf [https://perma.cc/53BN-G2V2] (reporting that the DJI Inspire is used by over two-hundred public agencies).

³¹² See, e.g., Luke Dormehl, *7 Drones that Can Stay Airborne for Hours—and the Tech that Makes It Possible*, DIGITAL TRENDS (Oct. 9, 2018, 11:29 AM), <https://www.digitaltrends.com/cool-tech/drones-with-super-long-flight-times> [https://perma.cc/M5JH-MN6F]. The maximum flight time of commercially available drones tends to be less than half an hour. See *id.*

³¹³ See *The 10 Longest Range Unmanned Aerial Vehicles (UAVs)*, AIR FORCE TECH. (June 19, 2019), <https://www.airforce-technology.com/features/featurethe-top-10-longest-range-unmanned-aerial-vehicles-uavs> [https://perma.cc/92YF-XL7T].

³¹⁴ See, e.g., Baude & Stern, *supra* note 45, at 1883; Jessica Dwyer-Moss, *The Sky Police: Drones and the Fourth Amendment*, 81 ALB. L. REV. 1047, 1056 (2018); Philip J. Hiltner, *The Drones Are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and Its Fourth Amendment Implications*, 3 WAKE FOREST J.L. & POL'Y 397, 404–09 (2013).

³¹⁵ Dwyer-Moss, *supra* note 314, at 1056; Farber, *supra* note 308, at 18–22; Hiltner, *supra* note 314, at 408.

³¹⁶ See Bennett, *supra* note 309 (describing the use of military-grade drones in domestic law enforcement). Note that FAA regulations prohibit the use of small drones during the night, although pilots can apply for waivers excepting them from this rule so long as they can demonstrate that the operation can be conducted safely. 14 C.F.R. §§ 107.29, 107.200, 107.205 (2017).

³¹⁷ See *Florida v. Riley*, 488 U.S. 445 (1989); *California v. Ciraolo*, 476 U.S. 207 (1986).

³¹⁸ See *infra* Appendix Table 1. Federal regulations set no minimum height for drone flights. See 14 C.F.R. § 107.1–107.205.

³¹⁹ 476 U.S. 207 (1986).

sidents' comings and goings, and their activities in their yards or adjacent fields, would be substantial. Moreover, the cost (especially the unit cost) of automated drone monitoring would be low, as the government would be able to efficiently gather a great deal of information without having to charter an airplane or operate a helicopter.

Because the government's surveillance would be moderately intimate, high in the amount of data gathered, and low in cost, it is likely that the Supreme Court would find it to be a search. There is a possibility that the Court would uncritically follow its manned overflight precedents and simply declare that any overflight observation is not a search.³²¹ But the fairly clear difference between automated drones and manned aircraft—and the Court's tendency to follow the intimacy, amount, and cost model in the vast majority of *Katz* test cases—suggests that this is improbable. The Court is likely to hold that prolonged video surveillance by drones is a search.

2. *Smart Homes and Devices*

"Smart" devices such as internet-connected watches, cars, clothes, medical devices, and home appliances generate a variety of information useful in criminal investigations.³²² In recent cases, the government has begun to use data from smart devices to establish defendants' guilt. James Bates was indicted for murder after data from his smart utility meter indicated that someone had used 140 gallons of water between 1 a.m. and 3 a.m., suggesting that he had hosed down a suspected murder scene.³²³ Prosecutors also obtained audio recordings made by Bates's Amazon Echo on the night in question.³²⁴ Ross Compton was charged with aggravated arson and insurance fraud based on data obtained from his pacemaker, which was inconsistent with his story of being awoken by a fire and climbing out of his bed-

³²⁰ *Id.* at 209 (during the investigation a "private plane . . . flew over" the defendant's house "at an altitude of 1,000 feet"); *Riley*, 488 U.S. at 448 (noting that a helicopter "circled" over the defendant's property "at the height of 400 feet").

³²¹ See *supra* note 315 and accompanying text.

³²² See Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 557–61 (2017) (describing various smart devices and police interest in the data they generate).

³²³ Haley Sweetland Edwards, *Alexa Takes the Stand: Listening Devices Raise Privacy Issues*, TIME (May 4, 2017), <http://time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues> [<https://perma.cc/4U9S-RLTW>].

³²⁴ *Id.* The charges against Bates were eventually dropped at the prosecutor's request. Nicole Chavez, *Arkansas Judge Drops Murder Charge in Amazon Echo Case*, CNN (Dec. 2, 2017, 12:52 AM), <https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html> [<https://perma.cc/2RE8-T2ZN>].

room window.³²⁵ Richard Dabate was charged with the murder of his wife after her Fitbit data showed her walking around an hour after Dabate claimed an intruder had killed her, and a key fob showed that Dabate was home after he had supposedly left for work.³²⁶

The use of data from smart devices inside the home (or inside Mr. Compton's chest) has raised concerns about the potential for the government to obtain data from such devices without any quantifiable suspicion of crime.³²⁷ Because consumers who interact with internet-connected devices almost inevitably disclose information to third party service providers, it remains ambiguous whether the Fourth Amendment will protect such information.³²⁸ This is true even after *Carpenter*, which limited the reach of the third-party doctrine but did so partly on the basis that cell phone users did not knowingly or voluntarily disclose their location information.³²⁹ An individual who uses a smart electricity meter or speaks to a smart speaker like an Amazon Echo is voluntarily disclosing information to a third party's servers, where it can be stored and analyzed.³³⁰ It is unclear whether the Fourth Amendment protects information intentionally disclosed to a third party.³³¹

The intimacy, amount, and cost model can shed light on the Fourth Amendment status of information voluntarily disclosed to a smart device. Assume that the government asks a smart speaker company to turn over all audio recordings made by a customer during the past four months. Like the Amazon Echo, the smart speaker at issue is always active but only stores and processes sound when the user speaks an activation word like "Alexa."³³² Thus, recordings are gener-

³²⁵ See Lauren Pack, *Arson Suspect in Unique Case Featuring Pacemaker Data Is Back in Custody*, JOURNAL-NEWS (July 24, 2018), <https://www.journal-news.com/news/arson-suspect-unique-case-featuring-pacemaker-data-back-custody/dn6JyzsOemZovpayJMZLNJ/> [<https://perma.cc/DLN5-XFGQ>].

³²⁶ Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You*, WASH. POST (Oct. 9, 2017), https://www.washingtonpost.com/local/public-safety/commit-a-crime-your-fitbit-key-fob-or-pacemaker-could-snitch-on-you/2017/10/09/f35a4f30-8f50-11e7-8df5-c2e5cf46c1e2_story.html [<https://perma.cc/ULC9-W8J8>].

³²⁷ See Ferguson, *supra* note 322, at 603; Dalmacio V. Posadas, Jr., *The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption*, 53 GONZ. L. REV. 89, 91 (2017).

³²⁸ See Ferguson, *supra* note 322, at 603.

³²⁹ 138 S. Ct. 2206, 2219–20 (2018).

³³⁰ See Raphael Davidian, *Alexa and Third Parties' Reasonable Expectation of Privacy*, 54 AM. CRIM. L. REV. ONLINE 58, 59–60 (2017).

³³¹ See *Carpenter*, 138 S. Ct. at 2219–20.

³³² See Davidian, *supra* note 330, at 59.

ally only made when the user directly and voluntarily conveys information to the device and the company's servers.³³³

The Supreme Court would likely hold that such a request for information was a Fourth Amendment search, despite the customer's voluntary disclosure of his information to a third party. The intimacy of the information sought is substantial, as it involves sound recordings of the inside of the customer's home, capturing not only his communications with the smart speaker but also any background noise or conversation occurring at the same time.³³⁴ The amount of information sought would be relatively high, potentially involving thousands of recordings made by the customer over the course of four months.³³⁵ And the cost of simply requesting such data, or even of issuing an administrative subpoena, would be relatively low.³³⁶

A similar analysis could be performed for a variety of related scenarios, such as recordings by a smart speaker installed in a car, data obtained from medical devices or smart clothing,³³⁷ and television viewing information recorded by smart televisions.³³⁸ Although the particular facts of the cases are difficult to predict with certainty, in general, those scenarios are likely to be deemed Fourth Amendment searches.

3. *Facial Recognition*

Facial recognition technology involves the use of software that compares the facial features of a person in a camera image to those in

³³³ It is possible that the smart speaker could mishear a word that sounds like the activation word and begin recording without the user's intent or knowledge. *See id.*

³³⁴ Cf. Matthew Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2134–36 (2009) (discussing the legal status of search terms).

³³⁵ It is likely that a court would know the precise quantity and size of the audio files requested from the smart speaker company when assessing a case like the one hypothesized here. If the actual amount of data that would be obtained is unknown, recall that it is ultimately the amount *sought* that drives the Court's reasonable expectations of privacy inquiry. In a rare case such as this one where the amount of data at issue is ambiguous, the Court is likely to use the potential amount of data captured as a proxy. The Court engaged in a similar analysis in *Carpenter*, where it emphasized the potential for tracking Carpenter's every movement over a five-year period rather than the actual tracking of his movements, which was far more limited. *See Carpenter*, 138 S. Ct. at 2218.

³³⁶ *See* David Kravets, *We Don't Need No Stinking Warrant: The Disturbing, Unchecked Rise of the Administrative Subpoena*, WIRED (Aug. 28, 2012, 6:00 AM), <https://www.wired.com/2012/08/administrative-subpoenas> [<https://perma.cc/4RMR-33Z4>].

³³⁷ *See* Jouvenal, *supra* note 326.

³³⁸ *See* Sapna Maheshwari, *How Smart TVs in Millions of U.S. Homes Track More Than What's on Tonight*, N.Y. TIMES (July 5, 2018), <https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html> [<https://perma.cc/TUF6-DWJ7>].

a database of known persons.³³⁹ By measuring characteristics like the shape of the person's nose and the distance between their eyes, it can identify a person based on their "faceprint."³⁴⁰ The accuracy of facial recognition technology is currently far from perfect, but it has improved rapidly over the past decade.³⁴¹

At present, law enforcement agencies largely use facial recognition technology to identify individuals from photographs taken in a controlled environment such as a police station.³⁴² But real-time facial recognition of individuals in public places has been adopted by some urban police departments, while others have expressed interest in purchasing such technology.³⁴³ The FBI has indicated that it is seeking the ability to recognize people in a crowd and track their movements during various events.³⁴⁴

Would the real-time use of facial recognition technology to identify and monitor attendees at a single public event be a Fourth Amendment search? So long as the Court considers the surveillance as an isolated act, it is unlikely to declare this a search. Suppose that the FBI scans a concert crowd for criminal suspects or other persons of interest, and in doing so identifies virtually every attendee as they enter and leave the venue. One of the concertgoers sues the government under Section 1983, claiming a violation of her Fourth Amendment rights.³⁴⁵ The intimacy of the data captured by the government's cameras would be relatively low. As the Supreme Court has said in a different context, a person's "facial characteristics" are not private or intimate and are constantly exposed to the public.³⁴⁶ Although the cost of identifying the individual concertgoer would be low, the amount of data captured involving the concertgoer is likewise low, comprising only two observations at a single public event. Given the non-intimate nature of the information and the low amount captured, it is unlikely that the Court would consider this a search.

³³⁹ Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1596 (2017).

³⁴⁰ Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 95 (2017).

³⁴¹ See *id.* at 95–96.

³⁴² See Hirose, *supra* note 339, at 1597.

³⁴³ *Id.*

³⁴⁴ See JENNIFER LYNCH, FACE OFF: LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY (Gennie Gebhart ed., 2018), <https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf> [<https://perma.cc/WH6G-KCNY>].

³⁴⁵ 42 U.S.C. § 1983 (2018).

³⁴⁶ *United States v. Dionisio*, 410 U.S. 1, 14 (1973).

This analysis might change, however, if the Court were to consider all of the other concertgoers along with the individual litigant. The total amount of information gathered from all affected persons would presumably be quite large.³⁴⁷ Nonetheless, the several “Fourth Amendment standing” cases prohibiting litigants from asserting the privacy rights of others suggest that the Court is unlikely to take this approach.³⁴⁸

Finally, the analysis would be very different if facial recognition technology became sufficiently pervasive as to allow the government to effectively track a person’s movements and location in public spaces over time.³⁴⁹ In that scenario, the intimacy, amount, and cost would be similar to that of a suspect whose car was tracked for 28 days using a GPS device. Such precise and ongoing location tracking would target somewhat intimate information, capture a relatively large amount of such information, and do so at a low cost. Pervasive and constant facial recognition tracking would thus likely be a search, for much the same reasons that other forms of location tracking were a search in *Jones* and *Carpenter*.³⁵⁰

CONCLUSION

The principles of intimacy, amount, and cost can lend coherence to Fourth Amendment law. Viewed through the lens of these principles, the reasonable expectation of privacy test is more consistent and predictable than is currently understood. Indeed, the principles-based model can help to explain the seemingly inexplicable course of the Court’s Fourth Amendment jurisprudence. Further, the model offers a unified conceptual framework, rather than the multiple, contradictory concepts that scholars have identified to date.

³⁴⁷ The Court briefly alluded to this aggregation concept in *United States v. Knotts* although it has not engaged in such an analysis to date. See 460 U.S. 276, 283–84 (1983) (suggesting that “if such dragnet-type law enforcement practices . . . should eventually occur” then the Court will examine whether it infringes on “constitutional principles”).

³⁴⁸ See, e.g., *Minnesota v. Carter*, 525 U.S. 83, 91 (1998) (applying a narrow concept of Fourth Amendment standing and affirming that a suspect could not assert the rights of the homeowner in whose house the suspect was temporarily located).

³⁴⁹ China, for instance, is seeking a similar form of pervasive video and facial recognition technology. See, e.g., Paul Mozur, *Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> [https://perma.cc/G2LT-8ZZC].

³⁵⁰ See *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018); *United States v. Jones*, 565 U.S. 400, 404–07 (2012) (holding the installation of a GPS device on a car intrudes into a person’s reasonable expectation of privacy by recording their every movement).

Whether the reasonable expectation of privacy test is the optimal way to determine the Fourth Amendment's scope will remain the subject of debate. It is possible that some alternative approach might be more accurate or capture a broader set of Fourth Amendment values.³⁵¹ What is clear is that current law would be substantially improved by greater recognition of the principles that appear to drive outcomes in the Supreme Court's Fourth Amendment cases. Overtly addressing these principles would enhance lower court assessments of Fourth Amendment privacy and provide the Supreme Court with thorough analyses to review and consider. Recognition of the principles would also improve societal understandings of the *Katz* test, offering a clear answer to the question of what violates a reasonable expectation of privacy. Further, the principles can provide a means for law enforcement officials and others to better predict whether novel surveillance techniques are likely to trigger the Fourth Amendment.³⁵² The time has come for the Supreme Court to overtly acknowledge the central importance of intimacy, amount, and cost to Fourth Amendment privacy.

³⁵¹ For some potential alternative approaches, see Brief of Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae in Support of Petitioner at 3, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530961; Baude & Stern, *supra* note 45, at 1825; Tokson, *supra* note 77.

³⁵² See *supra* Section IV.D.

APPENDIX

TABLE 1. REASONABLE EXPECTATION OF PRIVACY CASES AND THE INTIMACY, AMOUNT, AND COST OF SURVEILLANCE

Principles that indicate a search are shaded dark grey. Principles that indicate a non-search are shaded light grey. All principles were rated by multiple coders on an ordinal scale of one to seven.^a

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Katz v. United States , 389 U.S. 347, 348 (1967)	FBI agents attached a listening device to the outside of a phone booth and listened to Katz's conversations by activating the device when he approached the booth.	6	4	5	Search	
Terry v. Ohio , 392 U.S. 1, 7 (1968)	An officer patted down suspects for weapons.	6	1.5	2 ^b	Search	Intimacy ^c
Mancusi v. DeForte , 392 U.S. 364, 365 (1968)	State officials physically searched for and obtained papers from DeForte's shared office.	5	4.5	5	Search	
United States v. White , 401 U.S. 745, 746–47 (1971)	Officers recorded conversations between White and an informant in the informant's home and in four other locations. At the informant's house, one agent hid in a closet and another stood outside with a radio receiver.	6	5.5	7	No search (outlier)	
United States v. Dionisio , 410 U.S. 1, 3 (1973)	Dionisio challenged a grand jury subpoena directing him to give a voice exemplar.	1	1.5	3	No search	
United States v. Miller , 425 U.S. 435, 436 (1976)	The government served grand jury subpoenas for bank records at two of Miller's banks.	4	4	4	No search	Intimacy

^a Four coders separately coded each Fourth Amendment search case, assigning ratings for the intimacy, amount, and cost associated with the surveillance in each case. The numbers in Table 1 are the averages of the four coders' ratings. See *supra* notes 189–92 and accompanying text.

^b The cost measured here is that of the brief pat-down search, not the seizure that preceded it.

^c For excerpts of the discussions of intimacy, amount, and cost in these opinions, see *infra* tbl.2.

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Rakas v. Illinois, 439 U.S. 128, 130 (1978)	Police officers searched the interior of a car on suspicion of bank robbery. They discovered rifle shells in the glove box and a rifle under the passenger seat. The passengers moved to suppress the rifle and shells but did not claim ownership over the car or either item.	2 ^d	2.5	3	No search	
Smith v. Maryland, 442 U.S. 735, 735 (1979)	At police request, a telephone company installed a pen register on Smith's line for a day or two.	3	2	1.5	No search	Intimacy
Walter v. United States, 447 U.S. 649, 651-52, 655 n.6 (1980)	Several packages were mistakenly delivered to L'Eggs Products Inc. Employees opened the packages, finding therein boxes containing several copies of 25 different pornographic films. The employees did not view the films. They called the FBI, and FBI agents picked up the films and viewed them with a projector.	6	5	4.5	Search	

^d This inquiry is affected by standing doctrine, which does not allow the defendants to assert the interests of the car owner. To these passengers, the glove box and passenger compartment of a car owned and driven by someone else were not particularly intimate.

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
United States v. Payner, 447 U.S. 727, 729–30 (1980)	An IRS informant invited a Bahamas bank employee to dinner while another informant stole the employee's briefcase from the apartment where he was staying, opened the case, and gave the bank records to an IRS agent for photocopying. One of the bank's clients moved to suppress some of the documents.	2 ^e	4.5	7	No search	
Rawlings v. Kentucky, 448 U.S. 98, 100–01 (1980)	Police executing a warrant in Rawlings's house ordered a guest to empty out her purse, finding drugs that belonged to Rawlings. He moved to suppress them.	2 ^f	2.5	3	No search	Intimacy
United States v. Knotts, 460 U.S. 276, 277–79 (1983)	Police used an electronic beeper that emitted radio signals to help them track a container of chloroform that was transported via car, on public streets, to a cabin where drugs were being manufactured.	2.5	3	6.5	No search	Intimacy, Amount
Texas v. Brown, 460 U.S. 730, 733 (1983)	A police officer shined his flashlight into a car that he had lawfully pulled over.	2.5	2	2.5	No search	
United States v. Place, 462 U.S. 696, 698–99 (1983)	A dog trained to detect drugs sniffed around Place's luggage at an airport.	1 ^g	1	4	No search	Amount

^e This inquiry is affected by standing doctrine, which does not allow the defendant to assert the interests of the bank employee. To this defendant, a briefcase owned by someone else was not particularly intimate.

^f This inquiry is affected by standing doctrine, which does not allow the defendant to assert the interests of his guest. To this defendant, a purse owned by an acquaintance was not particularly intimate.

^g Note that the Court appears to analyze the dog sniff not as a physical inspection of the bag, but as a non-physical acquisition of information about the bag, based on an examination of the ambient air. *United States v. Place*, 462 U.S. 696, 707 (1983) (distinguishing the dog sniff from an inspection of the contents of the luggage and emphasizing the nature of the information collected as well as the “public place” where the inspection occurred).

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Illinois v. Andreas, 463 U.S. 765, 767–68 (1983)	Customs officials lawfully searched a shipping container and found a table containing marijuana inside. Police sealed the container and delivered it to Andreas. They then reopened the container without a warrant upon arresting Andreas.	2	2	5	No search	
Michigan v. Clifford, 464 U.S. 287, 290–91 (1984)	Arson investigators inspected a fire-damaged and uninhabited home. The home’s lower interior was extensively damaged, but some upstairs rooms (and the exterior) were largely undamaged. Personal belongings remained in the house and the Cliffords had arranged to have the house secured against intrusion in their absence.	6	6	5	Search	
United States v. Jacobsen, 466 U.S. 109, 111–12 (1984) – Issue 1	Federal Express employees searched a package damaged by a forklift and found baggies of white powder. They alerted the DEA. DEA agents removed the baggies from a tube inside the package.	2.5	2	3	No search	
United States v. Jacobsen, 466 U.S. 109, 111–12 (1984) – Issue 2	DEA agents then tested the white powder inside the baggies for cocaine.	1	1	2.5	No search	
Oliver v. United States, 466 U.S. 170, 173 (1984) – Issue 1	Police officers walked around a locked gate and past various “No Trespassing” signs and eventually onto Oliver’s property to observe Oliver’s secluded fields, where they saw marijuana.	3	3	4.5	No search	Intimacy

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Oliver v. United States, 466 U.S. 170, 174 (1984) – Issue 2	Police officers walked into the woods via a path between Thornton’s mobile home and another house. Thornton had placed “No Trespassing” signs around his property. The officers walked on the path, through the woods, until they reached two patches of marijuana plants, which they later learned were on Thornton’s property.	3	2	4	No search	Intimacy
United States v. Karo, 468 U.S. 705, 708, 712–13 (1984) – Issue 1	Police placed a beeper device in a can of ether and had a person sell it to Karo.	1	1	4	No search	
United States v. Karo, 468 U.S. 705, 709–10, 715 (1984) – Issue 2	The police used the beeper to verify that the can remained in a house in Taos, New Mexico.	4.5	3	3	Search	
United States v. Karo, 468 U.S. 705, 708–10, 720 (1984) – Issue 3	The police tracked the location of the can via visual surveillance and beeper monitoring while Karo transported the can on public roads from Albuquerque to Taos, with stops at various houses and storage facilities. The can eventually arrived at the house in Taos several months after its purchase.	3	5	6	No search	
United States v. Karo, 468 U.S. 705, 708–09, 720 (1984) – Issue 4	The police tracked the beeper while the can was stored in a warehouse storage facility, but the beeper was incapable of identifying the specific locker that contained the can.	2	2	3	No search	
Hudson v. Palmer, 468 U.S. 517, 519, 526 (1984)	Prison officials inspected Palmer’s prison cell and prison locker for contraband.	3.5	4	3	No search	

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Maryland v. Macon, 472 U.S. 463, 465, 467 (1985)	Undercover police officers entered an adult bookstore and purchased two magazines.	1.5	2	4	No search	
New York v. Class, 475 U.S. 106, 107–08, 114 (1986) – Issue 1	At a lawful traffic stop, a police officer visually observed the car's VIN number.	1	1	1.5	No search	
New York v. Class, 475 U.S. 106, 108 (1986) – Issue 2	At a lawful traffic stop, a police officer leaned in and reached into Class's car to move some papers in order to see the car's VIN number. In doing so, he saw the handle of a gun hidden under the driver's seat.	4	2	2	Search	
California v. Ciraolo, 476 U.S. 207, 209 (1986)	Police officer chartered a private plane and flew over Ciraolo's house at a height of 1,000 feet, where he and another officer identified marijuana plants in Ciraolo's back yard.	3.5	2.5	6.5	No search	
Dow Chemical Co. v. United States, 476 U.S. 227, 229 (1986)	The EPA hired a commercial aerial photographer to take precision aerial photographs of the 2,000-acre Dow Chemical facility in Midland, Michigan.	2	5	7	No search	Intimacy
Arizona v. Hicks, 480 U.S. 321, 323 (1987)	Police officers lawfully entered Hicks's apartment after a bullet was fired through its floor into the apartment below. One officer moved some stereo components in order to record their serial numbers.	3.5	1.5	2	Search (outlier)	
United States v. Dunn, 480 U.S. 294, 297–98 (1987)	Police officers entered Dunn's ranch property, avoiding his curtilage and crossing over several fences. Using flashlights, they observed a large barn while standing in the nearby field area.	4	3.5	4.5	No search	Intimacy

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
O'Connor v. Ortega, 480 U.S. 709, 712–13 (1987)	State hospital officials searched Dr. Ortega's office and desk, located in their hospital, while investigating misconduct charges.	6	5	4	Search	Intimacy
California v. Greenwood, 486 U.S. 35, 37–38 (1988)	A police officer asked the neighborhood garbage service to set aside Greenwood's trash bags and turn them over to her. The officer then searched through Greenwood's trash and found drug-related items.	4	4	5	No search	
Florida v. Riley, 488 U.S. 445, 448–49 (1989)	A sheriff's department official circled twice over Riley's property in a helicopter. He observed a greenhouse which was 10 to 20 feet behind Riley's mobile home, within the curtilage. The official, flying 400 feet above, observed marijuana in the greenhouse through a missing roof panel.	4 ^h	2	6	No search	Intimacy
Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 609–11 (1989) – Issue 1	The Federal Railroad Association promulgated regulations regarding drug testing of railroad employees. One regulation required collecting blood samples, at an independent facility, from employees after specified events, typically railroad accidents.	5	2	4 ⁱ	Search	Intimacy, Amount

^h Note that the police circled over and observed Riley's property as a whole, not just his greenhouse. *See* Florida v. Riley, 488 U.S. 445, 448 (1989).

ⁱ The Court appeared to analyze both the collection and the testing of the blood, and both are reflected in the assessments here. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616 (1989).

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Skinner v. Railway Labor Executives' Ass'n , 489 U.S. 602, 611 (1989) – Issue 2	Regulations also required or permitted performing a breathalyzer test following specified events or in response to suspicious behavior.	3	1	2	Search (outlier)	Intimacy, Amount
Skinner v. Railway Labor Executives' Ass'n , 489 U.S. 602, 611 (1989) – Issue 3	Regulations also required or permitted taking urine samples following specified events or in response to suspicious behavior.	5	2.5	3.5 ^j	Search	Intimacy
Minnesota v. Olson , 495 U.S. 91, 94 (1990)	Police entered Louanne Bergstrom's home to arrest Olson, who had stayed there as a guest overnight. They found Olson in an upstairs closet.	5	3	4	Search	
Minnesota v. Dickerson , 508 U.S. 366, 369 (1993)	A police officer performed a <i>Terry</i> stop of Dickerson. An ensuing pat-down revealed no weapons, but the officer felt a lump in a front pocket of Dickerson's nylon jacket. He probed and examined it with his fingers until he could ascertain that it was probably a bag containing drugs, at which point he put his hand in Dickerson's pocket and seized the bag.	6	2	2 ^k	Search	

^j The Court appeared to analyze both the collection and the testing of the urine, and both are reflected in the assessments here. *See id.* at 617.

^k This cost assesses the manual probing of the lump in Dickerson's pocket, not the cost of the seizure that proceeded it. *See Minnesota v. Dickerson*, 508 U.S. 366, 378 (1993).

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Minnesota v. Carter, 525 U.S. 83, 83, 85–86 (1998)	“A police officer looked in an apartment window through a gap in the closed blind” for several minutes “and observed respondents Carter and Johns and the apartment’s lessee bagging cocaine.” Carter and Johns had come to the apartment for the sole purpose of bagging cocaine and had been there for approximately 2.5 hours. They moved to suppress the cocaine.	3 ¹	2	3	No search	Intimacy
Bond v. United States, 529 U.S. 334, 334 (2000)	A border agent entered a Greyhound bus and squeezed the soft luggage that Bond had placed in the overhead bin.	5	3	2	Search	Intimacy
Ferguson v. City of Charleston, 532 U.S. 67, 69–71 (2001)	A state hospital established, in collaboration with the state police, a program of drug testing pregnant women’s urine without their knowledge or consent.	6	1.5	2.5	Search	
Kyllo v. United States, 533 U.S. 27, 30 (2001)	DOI agents used their thermal imager to scan Kyllo’s home for several minutes. The scan showed that an area of Kyllo’s house was hot and warmer than neighboring homes (which were also scanned), consistent with the use of halide marijuana grow lights.	5	2.5	4	Search	Intimacy

¹ This inquiry is affected by standing doctrine, which did not allow the defendants to assert the interests of the homeowner.

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Illinois v. Caballes, 543 U.S. 405, 406 (2005)	A dog trained to detect drugs sniffed around the outside of a car validly stopped for speeding.	1 ^m	1	3.5	No search	Amount
United States v. Jones, 565 U.S. 400, 403 (2012) (five Justices concur to say that this would be a search under the <i>Katz</i> test as well as a physical touching test)	FBI agents attached a GPS tracker to the undercarriage of a Jeep that Jones borrowed from his wife. The agents tracked Jones’s movements for 28 days.	5	6	3	Search	Intimacy, Amount, Cost
Maryland v. King, 569 U.S. 435, 440 (2013)	Upon King’s arrest, the police applied a cotton swab inside of his mouth for the purpose of collecting King’s DNA.	5	1 ⁿ	2	Search	
Byrd v. United States, 138 S. Ct. 1518, 1523 (2018)	Pennsylvania State Troopers pulled over the car Byrd was driving, but Byrd was not listed on the rental agreement of the car. The troopers searched the car and the trunk, where Byrd had stored personal effects.	4	4	3	Search	

^m Note that the Court appears to analyze the dog sniff not as a physical inspection of the car, but as a non-physical acquisition of information about the car, based on examination of the ambient air. *Illinois v. Caballes*, 543 U.S. 405, 409 (2005) (noting that the dog sniff did not go beyond the “the exterior of respondent’s car” and emphasizing the limited nature of the information obtained).

ⁿ Note that the Court’s assessment was simply of the cheek swab itself, not of the subsequent addition of that DNA to a database or the analysis of that DNA for matches to evidence from various crime scenes. *Maryland v. King*, 569 U.S. 435, 464 (2013). If that had been part of the analysis, the cost would be higher, but the amount of information obtained would also be higher (even from the non-coding DNA collected). *See, e.g.*, David Kaye, “*Open to Dispute*”: *CODIS STR Loci as Private Medical Information*, *FORENSIC MAG.* (May 28, 2014), <https://www.forensicmag.com/article/2014/05/open-dispute-codis-str-loci-private-medical-information> (noting that forensic DNA may correlate with diseases and may carry information about relatedness); Simon A. Cole, *Is the “Junk” DNA Designation Bunk?*, 102 *Nw. U. L. REV. COLLOQUY* 54, 59 (2007) (noting that forensic DNA may correlate with certain genetic diseases).

Case	Fact Summary	Intimacy	Amount	Cost	Case Outcome	Principles Discussed
Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) – Issue 1	Carpenter was suspected of involvement in various robberies in the Detroit area. Prosecutors obtained court orders under Section 2703(d) of the Stored Communications Act to obtain cell phone records for Carpenter and others. Sprint and Metro PCS disclosed these records. The first order sought 152 days of records.	5.5	7	2	Search	Intimacy, Amount, Cost
Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) – Issue 2	The second order sought seven days of records.	5	6	2	Search	Intimacy, Amount, Cost

TABLE 2. DISCUSSIONS OF INTIMACY, AMOUNT, OR COST IN
REASONABLE EXPECTATION OF PRIVACY OPINIONS

Case	Principles Discussed	Excerpted Discussion
Terry v. Ohio, 392 U.S. 1 (1968)	Intimacy	"[I]t is simply fantastic to urge that such a procedure performed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a 'petty indignity.' It is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly." 392 U.S. at 16–17 (footnote omitted).
United States v. Miller, 425 U.S. 435 (1976)	Intimacy	"On their face, the documents subpoenaed here are not respondent's 'private papers.' . . . The checks are not confidential communications but negotiable instruments to be used in commercial transactions. 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." 425 U.S. at 440–42.
Smith v. Maryland, 442 U.S. 735 (1979)	Intimacy	"Yet a pen register differs significantly from the listening device employed in <i>Katz</i> , for pen registers do not acquire the <i>contents</i> of communications. . . . 'Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.'" 442 U.S. at 741 (quoting <i>United States v. N.Y. Tel. Co.</i> , 434 U.S. 159, 167 (1977)).
Rawlings v. Kentucky, 448 U.S. 98 (1980)	Intimacy	"At the time petitioner dumped thousands of dollars worth of illegal drugs into Cox's purse, he had known her for only a few days. According to Cox's uncontested testimony, petitioner had never sought or received access to her purse prior to that sudden bailment." 448 U.S. at 105.

Case	Principles Discussed	Excerpted Discussion
United States v. Knotts, 460 U.S. 276 (1983)	Intimacy, Amount	“The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways. . . . ‘A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.’” 460 U.S. at 281 (quoting <i>Cardwell v. Lewis</i>, 417 U.S. 583, 590 (1974)). “Respondent . . . expresses the generalized view that the result of the holding sought by the government would be that ‘twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.’ . . . If such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.” <i>Id.</i> at 283–84 (citations omitted) (quoting Brief for Respondent at 9). “[T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.” <i>Id.</i> at 285.
United States v. Place, 462 U.S. 696 (1983)	Amount	“[T]he sniff discloses only the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited. . . . In these respects, the canine sniff is <i>sui generis</i>. We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure.” 462 U.S. at 707.
Oliver v. United States, 466 U.S. 170 (1984)	Intimacy	“[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields.” 466 U.S. at 179.
Dow Chemical Co. v. United States, 476 U.S. 227 (1986)	Intimacy	“It may well be . . . that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant. But the photographs here are not so revealing of intimate details as to raise constitutional concerns.” 476 U.S. at 238.
United States v. Dunn, 480 U.S. 294 (1987)	Intimacy	“It is especially significant that the law enforcement officials possessed objective data indicating that the barn was not being used for intimate activities of the home.” 480 U.S. at 302.

Case	Principles Discussed	Excerpted Discussion
O'Connor v. Ortega, 480 U.S. 709 (1987) (plurality)	Intimacy	"The undisputed evidence discloses that Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos." 480 U.S. at 718.
Florida v. Riley, 488 U.S. 445 (1989)	Intimacy	"As far as this record reveals, no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury. In these circumstances, there was no violation of the Fourth Amendment." 488 U.S. at 452.
Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989)	Intimacy, Amount	"In light of our society's concern for the security of one's person, it is obvious that this physical intrusion, penetrating beneath the skin, infringes an expectation of privacy that society is prepared to recognize as reasonable. The ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested employee's privacy interests. Much the same is true of the breath-testing procedures. . . . Subjecting a person to a breathalyzer test, which generally requires the production of alveolar or 'deep lung' breath for chemical analysis, implicates similar concerns about bodily integrity and, like the blood-alcohol test we considered in <i>Schmerber</i>, should also be deemed a search." 489 U.S. at 616–17 (citations omitted). "It is not disputed . . . that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic. Nor can it be disputed that the process of collecting the sample to be tested, which may in some cases involve visual or aural monitoring of the act of urination, itself implicates privacy interests. . . . "There are few activities in our society more personal or private than the passing of urine. Most people describe it by euphemisms if they talk about it at all. It is a function traditionally performed without public observation; indeed, its performance in public is generally prohibited by law as well as social custom.'" <i>Id.</i> at 617 (quoting <i>Nat'l Treasury Emps. Union v. Von Raab</i>, 816 F.2d 170, 175 (1987)). "[B]reath tests reveal the level of alcohol in the employee's bloodstream and nothing more. Like the blood-testing procedures mandated by Subpart C, which can be used only to ascertain the presence of alcohol or controlled substances in the bloodstream, breath tests reveal no other facts in which the employee has a substantial privacy interest." <i>Id.</i> at 625–26.

Case	Principles Discussed	Excerpted Discussion
Minnesota v. Carter, 525 U.S. 83 (1998)	Intimacy	“Property used for commercial purposes is treated differently for Fourth Amendment purposes from residential property. . . . the purely commercial nature of the transaction engaged in here, the relatively short period of time on the premises, and the lack of any previous connection between respondents and the householder, all lead us to conclude that respondents’ situation is closer to that of one simply permitted on the premises.” 525 U.S. at 90–91.
Bond v. United States, 529 U.S. 334 (2000)	Intimacy	“Physically invasive inspection is simply more intrusive than purely visual inspection. . . . Although Agent Cantu did not ‘frisk’ petitioner’s person, he did conduct a probing tactile examination of petitioner’s carry-on luggage. Obviously, petitioner’s bag was not part of his person. But travelers are particularly concerned about their carry-on luggage; they generally use it to transport personal items that, for whatever reason, they prefer to keep close at hand.” 529 U.S. at 337–38.
Kyllo v. United States, 533 U.S. 27 (2001)	Intimacy	“In the home, our cases show, <i>all</i> details are intimate details, because the entire area is held safe from prying government eyes.” 533 U.S. at 37.
Illinois v. Caballes, 543 U.S. 405 (2005)	Amount	The dog sniff “discloses only the presence or absence of narcotics. . . . drug sniffs are designed, and if properly conducted are generally likely, to reveal only the presence of contraband.” 543 U.S. at 409.

Case	Principles Discussed	Excerpted Discussion
United States v. Jones, 565 U.S. 400 (2012)	Intimacy, Amount, Cost	“GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: ‘limited police resources and community hostility.’” 565 U.S. at 415–16 (Sotomayor, J., concurring) (citations omitted) (quoting <i>Illinois v. Lidster</i>, 540 U.S. 419, 426 (2004)). “The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may ‘alter the relationship between citizen and government in a way that is inimical to democratic society.’” <i>Id.</i> at 416 (quoting <i>United States v. Cuevas-Perez</i>, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). “In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.” <i>Id.</i> at 429 (Alito, J., concurring) (footnote omitted). “[S]ociety’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.” <i>Id.</i> at 430.

Case	Principles Discussed	Excerpted Discussion
Carpenter v. United States, 138 S. Ct. 2206 (2018)	Intimacy, Amount, Cost	“Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.” 138 S. Ct. at 2216. “Mapping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts.” <i>Id.</i> at 2217. “As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’ These location records hold for many Americans the ‘privacies of life.’ And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.” <i>Id.</i> at 2217–18 (citations omitted) (quoting <i>Jones</i>, 565 U.S. at 415 (Sotomayor, J. concurring) and <i>Riley v. California</i>, 573 U.S. 373, 403 (2014)). “A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” <i>Id.</i> at 2218. “Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government’s view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.” <i>Id.</i> “Yet this case is not about ‘using a phone’ or a person’s movement at a particular time. It is about a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in <i>Smith</i> and <i>Miller</i>.” <i>Id.</i> at 2220.