The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data After Carpenter

Michael Gentithes
Visiting Assistant Professor Chicago-Kent College of Law

THE END OF *MILLER*'S TIME: HOW SENSITIVITY CAN CATEGORIZE THIRD-PARTY DATA AFTER *CARPENTER*

Michael Gentithes[*]

For over 40 years, the Supreme Court has permitted government investigators to warrantlessly collect information that citizens disclose to third-party service providers. That third-party doctrine is under significant strain in the modern, networked world. Yet scholarly responses typically fall into unhelpfully extreme camps, either championing an absolute version of the doctrine or calling for its abolition. In Carpenter v. United States*, the Court suggested a middle road, holding that some categories of data—such as digital location information collected from cell phones—do not neatly fall into the third-party doctrine's dichotomy between unprotected, disclosed information and protected, undisclosed information. But the majority elucidated little rationale upon which to draw such nuanced distinctions.*

This Article provides the missing rationale for such categorization: informational sensitivity. Disclosure to a third party matters but is not a trump card. Sensitivity matters too. I thus propose a two-step test to determine if the government must obtain a warrant before collecting information from a third party. First, the Court should analyze the information's sensitivity, placing it on a sensitivity continuum rather than a disclosure dichotomy. The Court can look to related jurisprudence, and the inherent meaning such information conveys, to determine placement on that continuum. Second, if the

[*] Visiting Assistant Professor, Chicago-Kent College of Law. I am extremely grateful for the comments of Barry Friedman, Harold Krent, Carolyn Shapiro, Christopher Schmidt, Andy Grewal, Mark Rosen, Lori Andrews, Elizabeth De Armond, Anthony Michael Kreis, Alexander Boni-Saenz, Nancy Marder, Adrian Walters, Cody Jacobs, Kent Streseman, Kimberly Bailey, Richard Wright, Greg Reilly, Martin Malin, and Priyanka Bhattacharya.

information is sensitive, the Court should decide whether the government has collected enough of it to create an informational mosaic of the citizen. If so, that collection is a search.

The Court has long held that some data, like medical records or phone conversations, are too sensitive to be warrantlessly collected from third parties. Intermediately sensitive data, like the financial information in United States v. Miller *and the cell site location information in* Carpenter*, might be warrantlessly collected in small amounts, but is too sensitive for warrantless collection in bulk. The Court should adjust the third-party doctrine to account for such sensitive information and craft provisional rules to protect it. Doing so will enhance both the public's security and its regard for the Court.*

TABLE OF CONTENTS

INTRODUCTION

For over four decades, Supreme Court precedent has suggested that when citizens disclose information to any non-governmental third party, they relinquish their expectation that the information is private—and hence relinquish any Fourth Amendment rights—no matter how sensitive that information may be.[1] The most influential case creating that third-party doctrine, *United States v. Miller*, established that government investigators can warrantlessly gather unlimited financial data from bankers to whom citizens have disclosed it.[2] The doctrine has come under significant strain in today's networked world, as the recent *Carpenter v. United States* litigation has shown.[3] Yet scholarly views on the third-party doctrine have not adequately responded, mostly falling into unhelpfully extreme camps. The doctrine's champions claim that it should mean just what it says: citizens relinquish any expectation of privacy, and hence any Fourth Amendment protection, in information they willingly disclose to third parties.[4] Abolitionists respond that the third-party doctrine is

---

[1] The Justices have held that

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

United States v. Miller, 425 U.S. 435, 443 (1976).

[2] *Id.* at 446. Three years later, the Court expanded the doctrine to include far less sensitive information—the phone numbers citizens dial from their home telephone. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).

[3] 138 S. Ct. 2206, 2214 (2018) ("This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents.").

[4] Orin Kerr describes this as the "eyewitness rule"—the idea that there is no Fourth Amendment right preventing others from telling the government what they have seen or heard about you. *See* Orin Kerr, *Symposium:* Carpenter *and the Eyewitness Rule*, SCOTUSBLOG, (Aug. 4, 2017, 1:39 PM), http://www.scotusblog.com/2017/08/symposium-carpenter-eyewitness-rule/ ("One of the most basic ideas in Fourth Amendment law is what you might call the eyewitness rule: The government can always talk to eyewitnesses. If the police find out a bank was robbed, they can go to the bank and interview those who saw the crime occur. They can talk to the bank clerk about what he observed. They can talk to the security guard about what she experienced. They can talk to bank customers about what happened. These interviews, whether voluntary or compelled, don't trigger the Fourth Amendment. There's just no Fourth Amendment right to prevent people from talking about

an aberration that should be overruled in its entirety.[5] According to abolitionists, citizens do not voluntarily convey data to third parties nor do they assume the risk that a third party will disclose it to inquiring investigators, because citizens must use many third-party services—like banking and telecommunications—just to survive in the modern world.[6]

In the Court's most recent term, a majority of the Justices favored a categorical approach to data disclosed to third parties.[7] The *Carpenter* majority suggested that some categories of data—such as digital location information collected from cell phones—do not neatly fall into the third-party doctrine's dichotomy between unprotected, disclosed information and protected, undisclosed information.[8] But the majority elucidated little rationale, beyond

---

what they saw you do."). The ABA's proposed standards on law enforcement access to third party records also highlight the resonance of the third-party rationale: "Privacy is a divisible commodity, meaning information often retains some degree of privacy despite being shared. Nonetheless, disclosures can affect privacy. . . . [W]hat is given to even one person or entity is more likely to be further disseminated than before." ABA STANDARDS FOR CRIMINAL JUSTICE, LAW ENFORCEMENT: ACCESS TO THIRD PARTY RECORDS § 25-4.1(a) cmt. (3d ed. 2013) [hereinafter ABA STANDARDS] (citations omitted).

[5] *See* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 13 (2012) ("[T]he most egregious aspect of the third-party doctrine [is] its immunization of governmental acquisition of personal information held by third parties." (citations omitted)).

[6] As I argue in Part II.A below, this critique of the assumption of the risk rationale has a long lineage extending from the dissents in the original third-party-doctrine cases to modern Fourth Amendment scholarship. *See, e.g.*, *Miller*, 425 U.S. at 448–51 (Brennan, J., dissenting); *Smith*, 442 U.S. at 749–50 (1979) (Marshall, J., dissenting); *see also* ABA STANDARDS, *supra* note 4, at § 25-4.1(a); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 267 (2016) ("It is . . . impossible to fully participate in modern economic life without involving a bank to execute transactions. Because this third-party interaction is unavoidable, it undermines the assumption of risk rationale."); Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J., Aug. 2012, http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/. ("The reality is quite different, though, almost akin to compelled consent, which is not consent at all. If you want to communicate efficiently today, your communications likely will go through your ISP's servers. The alternative means of communication either involve conveying information to other third parties, or traveling to the other communicant so you can have a personal chat. Consent in this context has little meaning.").

[7] *Carpenter*, 138 S. Ct. at 2216–17 ("[W]hile the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records.").

[8] *See id.* at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome

the Justices' intuitions, upon which to draw such nuanced categorical distinctions.[9]

This Article provides that missing rationale. I chart a middle course between the champions and the abolitionists of the third-party doctrine, one that helpfully supplements the Court's categorical approach.[10] While disclosed information receives less Fourth Amendment protection, disclosure is not a trump card.[11] My

---

Carpenter's claim to Fourth Amendment protection."). The varied dissents in *Carpenter*, on the other hand, alternately decried and celebrated that doctrine's death. *See id.* at 2230 (Kennedy, J., dissenting) (claiming that the majority "misreads this Court's precedents, old and recent, and transforms *Miller* and *Smith* into an unprincipled and unworkable doctrine," creating a "newly conceived constitutional standard [that] will cause confusion; will undermine traditional and important law enforcement practices; and will allow the cell phone to become a protected medium that dangerous persons will use to commit serious crimes"); *id.* at 2263 (Gorsuch, J., dissenting) (arguing that citizens "often *do* reasonably expect that information they entrust to third parties . . . will be kept private," and that the Court "has never offered a persuasive justification" for the third-party doctrine's contrary holding).

[9] As Justice Kennedy's dissent highlighted, the majority offered only a "multifactor analysis . . . considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness," which he labeled an "unstable foundation" for a categorical approach to the Fourth Amendment protection afforded to information disclosed to third parties. *Id.* at 2234 (Kennedy, J., dissenting).

[10] *See id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronical of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.").

[11] The champions' view focuses too narrowly upon the guilty criminals that are the subject of most Fourth Amendment litigation and the police officers who pursue them. Unlike many of the Constitution's criminal protections, which are expressly provided to individual defendants, the Fourth Amendment focuses on "the people," who are guaranteed "the right . . . to be secure in their persons, houses, papers, and effects." U.S. CONST. amend IV. *See also* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 142–43 (2012) ("The aim of the Fourth Amendment is. . . the preservation of a vibrant society that respects the freedom and autonomy of each individual."); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 120 (2008) ("But in the Fourth Amendment, the rightholders are the *people*. . ." (emphasis in original)). As I discuss more below in Part IV, some current Fourth Amendment scholarship misleadingly suggests that Fourth Amendment jurisprudence is a series of adjustments to ensure a consistent degree of difficulty for cops uncovering crime. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 486 (2011) (arguing that new technologies "threaten the privacy/security balance because they enable both cops and robbers to accomplish tasks they couldn't before, or else to do old tasks more easily or cheaply than before"); *see also* Michael Gentithes, *Tranquility & Mosaics in the Fourth Amendment: How Our Collective Interest in Constitutional Tranquility Renders Data Dragnets Like the NSA's Telephony Metadata Program a Search*, 82 TENN. L. REV. 937, 948 (2015). But as the Supreme Court has acknowledged, Fourth Amendment doctrine protects

proposal builds upon earlier efforts to establish a sliding scale of Fourth Amendment protection, but deemphasizes empirically-measured views of privacy or legislative responses to government investigatory techniques.[12] Instead, I employ the concept of informational sensitivity to suggest that the third-party doctrine should allow for moderate protection for much of the information we commonly disclose to third parties. Using that approach, the Court should end *Miller*'s time as an absolutist precedent granting warrantless access to sensitive information like our financial records in any form or quantity.[13]

I propose a two-step test to determine whether the government must obtain a warrant to collect particular categories of information from a third party. In the first step, the Court should analyze that information's sensitivity, placing it on a sensitivity continuum rather than a dichotomy between disclosed and undisclosed data. The Court can look to related jurisprudence, and the inherent meaning such information conveys, to determine placement on the sensitivity continuum. For instance, *Miller*'s financial information and *Carpenter*'s cell site location information (CSLI) should be intermediate points on that continuum because (1) the Court has discussed how sensitive those categories of information are in related cases and (2) that information conveys significant substantive meaning on its face.[14] While disclosed metadata is not

---

"the innocent and guilty alike." Draper v. United States, 358 U.S. 307, 314 (1959) (Douglas, J., dissenting). *See generally* Riley v. California, 134 S. Ct. 2473 (2014); Gentithes, *supra*.

[12] *See infra* Part II.B (discussing the ABA STANDARDS, *supra* note 4). For additional sliding scale approaches to the Fourth Amendment, see Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 621–22 (2017); Price, *supra* note 6, at 268–69.

[13] *See* SCHULHOFER, *supra* note 11, at 121 ("'Modernization' cannot be a one-way street where the government benefits from new technologies while citizens are left with no protective buffers other than those that sufficed in 1791—the roofs, walls, and sealed envelopes that afforded complete privacy in the eighteenth century.").

[14] *See Carpenter*, 138 S. Ct. at 2217 (emphasizing the intimate window that CSLI provides into a customer's life and insisting that its "unique nature" requires categorization outside of the third-party doctrine's strict dichotomy). These statements hint at the importance of the inherent meaning that information facially conveys when categorizing that information for third-party doctrine purposes. Additionally, at the time *Carpenter* was decided, the Court's prior jurisprudence strongly suggested that long-term location information might be particularly sensitive. *See, e.g.*, *Riley*, 134 S. Ct. at 2490 ("Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations

sensitive and may be subject to warrantless collection in bulk, disclosed information with an inherent magnitude of sensitivity merits further scrutiny.[15]

In the second step, the Court should decide whether the government has collected enough sensitive information to create an informational mosaic of the citizen, thereby conducting a search.[16] A citizen has a small but cognizable expectation of privacy[17] in each such sensitive datum that a third party collects. Although government collection of one or even several of those data points may not raise constitutional concerns, if the government collects enough of them, the data points create such a detailed picture of the citizen's life that the government has conducted a search for which it must usually obtain a warrant.[18]

---

of most offenses impinges on expectations of privacy."). As I discuss in more detail in Part IV below, these nuggets of related jurisprudence suggest the sensitivity of location information. See Parts II.C & II.D for a more detailed explanation of how the Court should determine sensitivity and additional examples.

[15] *See, e.g.*, *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about [his or her] familial, political, professional, religious, and sexual associations"); *see also* SCHULHOFER, *supra* note 11, at 129 ("[R]outing information in our email is the functional equivalent of the telephone numbers that current Fourth Amendment law does not protect. But the *content* of our email is the functional equivalent of the content of a phone conversation. On any sensible approach to communications privacy, email content and telephone content should have identical protection." (emphasis in original)). *But see* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1020–21 (2010) (arguing that email addressing information does not convey content and is therefore not protected by the Fourth Amendment.). As I discuss in Part II.B below, this open acknowledgement that unlimited collection of some categories of non-sensitive data does not run afoul of the Fourth Amendment also distinguishes my approach from other efforts to measure the "privacy" of information on a sliding scale, such as the ABA's proposed standards on law enforcement access to third party records. *See generally* ABA STANDARDS, *supra* note 4.

[16] *See, e.g.*, Katz v. United States, 389 U.S. 347, 360 (1967) (establishing the modern test for what constitutes a search under the Fourth Amendment).

[17] *See id.* at 361 (1967) (Harlan, J., concurring) (arguing that proving a governmental intrusion into one's reasonable expectation of privacy is "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

[18] For more general background on the mosaic theory of the Fourth Amendment, see David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 68–69 (2013); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012). My position here is also consistent with my earlier work on the mosaic theory of the Fourth Amendment and constitutional tranquility, as I discuss in Part II.B below. *See* Gentithes, *supra* note 11, at 960–65.

My proposal accommodates the doctrine's limits that the Court has long tacitly accepted and recently aimed to formalize.[19] While telephone numbers delivered to a third-party telephone company are wholly unprotected under the Fourth Amendment, other information revealed to third parties, like medical information,[20] the content of a conversation,[21] or CSLI,[22] are protected. Some types of data are inherently sensitive, such as internet search histories, collections of photographs, and—despite the holding in *Miller*—financial information.[23] Following its instincts in these cases, the Court should adjust the third-party doctrine, dissolve the false dichotomy between disclosed and undisclosed data, and offer limited protection to categories of sensitive information even if they are given to third parties.

Stare decisis does not require the Court to blindly uphold *Miller*. Third-party-doctrine cases examine the constitutionality of new law enforcement efforts to gather information about suspects over an extended timeline. Such cases consider technological advances that were unimaginable just years earlier.[24] Because of those challenges, third-party cases should be viewed as a series of provisional prescriptions to which stare decisis does not fully apply. Citizens deserve, and the Court should not hesitate to craft, a reimagined Fourth Amendment that provides some protection to the sizeable caches of sensitive information that citizens regularly convey to third-party service providers while performing mundane tasks.[25]

In Part I below, I explain how the Court created the current third-party doctrine, with emphasis on how it later tacitly

---

[19] *See infra* Part II.B.

[20] *See infra* notes 74–76 and accompanying text..

[21] *See infra* note 73 and accompanying text.

[22] *See infra* notes 77–79 and accompanying text.

[23] *See* Riley v. California, 134 S. Ct. 2473, 2489–90, 2493 (2014). As I discuss in more detail in Part II.D.1 below, the Court's First Amendment jurisprudence also suggests that financial information is particularly sensitive as a form of constitutionally-protected free speech. *See* Buckley v. Valeo, 424 U.S. 1, 16–20 (1976).

[24] For a discussion of some of those emerging technologies, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 192–94 (2007).

[25] Reimagining the third-party doctrine will give the Court the flexibility it needs to address government acquisition of third-party records generated by new technologies, such as the CSLI at issue in *Carpenter*. 138 S. Ct. at 2219. As I explain in more detail in Part IV below, the Court has tacitly acknowledged that detailed records of a person's public and private locations raise heightened Fourth Amendment concerns.

acknowledged the doctrine's limitations.[26] I then argue for an end to *Miller*'s time in Part II.[27] While champions correctly note that a citizen's disclosure of information to a third party is constitutionally relevant, abolitionists rightly respond that the doctrine must be reworked given the modern ubiquity of data disclosures to third-party service providers.[28] The Court should dissolve *Miller*'s false dichotomy of disclosed and undisclosed third-party information, replacing it with a two-step test informed by the sensitivity of that information.[29] In Part III, I explain that the Court can adjust the third-party doctrine without offending principles of stare decisis, because the doctrine, like much of Fourth Amendment jurisprudence based upon contingent privacy expectations, is necessarily provisional.[30] Finally, in Part IV, I explain how informational sensitivity supplies the missing rationale for the Court's categorical approach in *Carpenter*. By applying that rationale, the Court can excise *Miller* and chart a clear course forward for third-party cases.[31]

I. THE FOURTH AMENDMENT'S PATH TO *MILLER*

The Fourth Amendment to the United States Constitution provides "the people" the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[32] It is thus a uniquely public-facing criminal procedure protection. Unlike the Fifth and Sixth Amendment protections, which are expressly directed towards individual defendants, the Fourth Amendment grants an inviolable right to all citizens, not just those suspected of or charged with crimes.[33] "The aim of the Fourth

---

[26] *See infra* Part I.

[27] *See infra* Part II.

[28] *See infra* Parts II.A and II.B.

[29] *See infra* Parts II.C and II.D.

[30] *See infra* Part III.

[31] *See infra* Part IV.

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

[33] *See* Rubenfeld, *supra* note 11, at 120 ("The Fourth Amendment differs in an important respect from the criminal procedure guarantees that immediately follow it. In the Fifth Amendment, the rightholder is expressly made singular: 'nor shall any *person* be . . . compelled in any criminal case to be a witness against *himself*.' Similarly, the Sixth Amendment's rights bearer is the singular 'accused,' who is granted, for example, the right 'to be confronted with the witnesses against *him*.' But in the Fourth Amendment, the rightholders are the *people*, who are 'to be secure in *their* persons, houses, papers, and effects.'

Amendment is different—the preservation of a vibrant society that respects the freedom and autonomy of each individual."[34] Fourth Amendment holdings are "for the innocent and guilty alike," protecting them all from invasions of their privacy and tranquility.[35]

The Supreme Court has struggled to define that broadly-granted right. One challenge is determining what government activities constitute an "unreasonable search and seizure" that government investigators can conduct only after they obtain a warrant. The Court has constructed a number of analytical artifices atop the sparse text in an effort to answer that challenge.

The most important analytical device the Court employs is the reasonable expectation of privacy (REOP) test.[36] As I have outlined elsewhere,[37] though the Court's early definitions of a "search" emphasized the amendment's relationship "to common-law trespass,"[38] the Court's focus slowly transformed throughout the 20th century into its present-day emphasis on "people, not places."[39] In his dissent in *Olmstead v. United States*, Justice Brandeis highlighted that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[40]

Brandeis's views were partially formalized nearly forty years later in *Katz v. United States*, a case concerning an eavesdropping

---

It is not only security, but 'the right *of the people* to be secure' that vanishes when the Fourth Amendment is read simply to prohibit 'unreasonable searches and seizures.'" (emphasis in original) (citations omitted)).

[34] SCHULHOFER, *supra* note 11, at 142.

[35] Draper v. United States, 358 U.S. 307, 314 (1959) (Douglas, J., dissenting); *see* Riley v. California, 134 S. Ct. 2473, 2492 (2014); Gentithes, *supra* note 11, at 939 ("[M]illions of Americans share a joint Fourth Amendment interest in constitutional tranquility. . . .").

[36] Katz v. United States, 389 U.S. 347, 350–51 (1967).

[37] *See* Gentithes, *supra* note 11, at 941–44.

[38] United States v. Jones, 565 U.S. at 405 (2012). An example of a case that used the common-law trespass rationale is *Olmstead v. United States*, which held that taps attached to telephone wires in public streets did not run afoul of the Fourth Amendment simply because none of the material things mentioned in the amendment—a citizen's person, house, papers or effects—were intruded upon by the government's action. 277 U.S. 438, 463–64 (1928), overruled by *Katz*, 389 U.S. at 350–51.

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

[40] 277 U.S. at 478 (Brandeis, J., dissenting); *see also* Scott E. Sundby, *'Everyman's' Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1755–56 (1994) (emphasizing the importance of the founding principles of the Fourth Amendment that Brandeis elucidated in his dissent).

device attached to a public telephone booth.[41] In a concurrence that the Court has since applied to innumerable cases, Justice Harlan suggested that government conduct amounts to a search triggering the Amendment's protections when it intrudes upon a citizen's "constitutionally protected reasonable expectation of privacy."[42] Harlan said that in order for a citizen to demonstrate that government conduct has intruded upon such a reasonable expectation of privacy, she must in turn meet "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[43]

The REOP test is now the touchstone in determining whether government conduct constitutes a search. Through the REOP test, the Court can preserve traditional zones of privacy in the face of new governmental investigative techniques. As Eleventh Circuit Judge Robin S. Rosenbaum adeptly described:

> [E]xisting Supreme Court precedent may fairly be construed to suggest that where society has historically recognized a legitimate expectation of privacy, we must continue to do so for purposes of Fourth Amendment analysis, even if, in our modern world, we must now expose to a third party information that we would have previously kept private, in order to continue to participate fully in society. If we do not, we will face the Hobson's choice of leaving our historically recognized Fourth Amendment rights at the door of the modern world or finding ourselves locked out from it. That the Constitution will not abide.[44]

---

[41] 389 U.S. at 347.

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

[43] *Id.* at 361. Others have argued that modern employment of the REOP test has eliminated the subjective prong, rendering the test wholly objective. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113–14 (2015).

[44] United States v. Davis, 785 F. 3d 498, 527 (11th Cir. 2015) (Rosenbaum, J., concurring); *see also* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public,* 66 EMORY L. J. 527, 577 (2015).

As an analytical device, the REOP test is only equipped to check new government search techniques based upon judges' rough, current impressions of what privacy protections are important enough to maintain for the foreseeable future.[45] It cannot be read literally as an empirical measure of all citizens' understandings of how technology functions, and thus what information the government can reasonably, warrantlessly obtain at any given moment.[46] There may be a "correct" answer to that inquiry, but it is impossible to determine. Citizens vary widely in their mastery of new technology, and their understandings are in flux as they obtain new information or as new publicity about technological capabilities emerges.[47] The only "correct" answer would have to be derived from

---

[45] As I discuss in more detail below, the Justice's rulings in third-party-doctrine cases should be considered especially provisional. *See infra* Part III.

[46] *See* Carpenter v. United States, 138 S. Ct. 2206, 2245 (2018) (Thomas, J., dissenting) (discussing the circularity of a test that asks a descriptive question about society's expectations to answer a question that will actually shape those very expectations); SCHULHOFER, *supra* note 11, at 121 ("Existing expectations are shaped by the police practices that the law allows. If we decide what the law allows by looking to existing expectations, we end up chasing ourselves in a circle. Inescapably, decisions interpreting the Fourth Amendment determine what kind of privacy we are *entitled* to expect." (emphasis in original)); Rubenfeld, *supra* note 11, at 106 ("The threat of circularity. . . is easy to see. Suppose the President announces that all telephone conversations will henceforth be monitored. Arguably, no one thereafter can reasonably expect privacy in his phone calls, and the announced eavesdropping will have constitutionalized itself. The same problem will afflict legislative and judicial pronouncements about police searches or seizures.").

[47] *See* Matthew Tokson, *Knowledge and the Fourth Amendment*, 111 NW. U. L. REV. 139, 188 (2016).

> Societal knowledge is a complex, multilayered concept that does not lend itself to easy application in criminal cases. Knowledge typically spreads unevenly through the population, and attributing median societal knowledge to criminal defendants raises questions of fundamental fairness. Judges are societal elites who are systematically likely to overestimate the extent of societal knowledge . . . . Further, even if societal knowledge could be measured perfectly, anchoring the Fourth Amendment's scope to it will lead to a gradual erosion of Fourth Amendment protection. As an increasingly intelligent and educated population gains awareness and understanding of new technologies and threats to privacy, expectations of privacy and the sphere of Fourth Amendment protection will naturally shrink.

See also United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."); Levinson-Waldman, *supra* note 44, at 550 ("[T]echnology itself—its ubiquity, and its convenience—can dynamically change [society's] expectations. As people become more reliant . . . technology may seem less intrusive, making the apparent privacy risks recede as well. A test premised on the reasonable expectation of privacy must become more objective to account for that shift.").

a snapshot of all citizens at precisely the same time. Even if judges could capture such a snapshot, a majority of popular expectations is an inappropriate baseline for Fourth Amendment line-drawing.[48] The Bill of Rights often protects minorities by limiting the majority's will.[49] The Fourth Amendment is no different; it aims to protect "dissidents and social outcasts" and "must not be read to permit whatever intrusions are acceptable to those in the conventional mainstream."[50]

Furthermore, any snapshot of citizens' understandings and expectations may be subject to undue influence from the government itself, which could massively publicize its intent to regularly invade spheres of life previously considered private.[51] And society's understanding of what is reasonable changes as citizens decide whether the capabilities of a new technology are worth the tradeoff in how that technology reduces our privacy, giving the Court a moving target.[52]

Because the society-wide aspects of the REOP test are unstable and perhaps unknowable, the Court's implementations of it merely

---

[48] *See* SCHULHOFER, *supra* note 11, at 141 ("The major aim of the Fourth Amendment—unquestionably— is not to bolster majority rule but to afford shelter to political, religious, and ideological minorities.").

[49] *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C.L. REV. 1511, 1522 (2010) ("[V]arious subgroups may differ in their attitudes about privacy. People's attitudes about privacy diverge depending upon their race, ethnicity, or religion. The Bill of Rights has oft been championed as necessary to protect minorities by limiting the will of the majority. [Using empirical evidence to identify reasonable expectations of privacy] would make the Fourth Amendment too shackled to the preferences of the majority. Moreover, it would strike many as illegitimate because the Constitution is supposed to transcend the will of the majority at any particular moment in time.").

[50] *See* SCHULHOFER, *supra* note 11, at 120 (arguing that judges and academics should not look to mainstream public opinion to decide what reasonable expectations of privacy are).

[51] *See* Solove, *supra* note 49, at 1524 ("[T]he government could condition the populace into expecting less privacy. For example, . . . the government could diminish expectations of privacy by announcing on television each night that we could all be subject to electronic surveillance." (citation omitted)); *see also* Levinson-Waldman, *supra* note 44, at 552 ("*Katz*'s approach can also put the government in an enviable position: when a technology is first introduced, it is new, it is experimental . . . . By the time the technology is in place and publicly revealed, and society has begun to grasp its true implications, it is too late; only an out-of-tough Luddite could be said not to understand, and implicitly consent to, all its potential uses. For the government, it is heads, we win; tails, you lose.").

[52] *See* United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

freezes privacy protections that the Justices deem important enough to maintain for the foreseeable future. If the Court finds a reasonable expectation of privacy, it means only that its sense of what has been reasonable until today shall remain reasonable going forward—even if technology continues to advance.[53] Such judicial estimations provide needed flexibility for Justices aiming to uphold privacy in the face of monumental advances in technology.

A. DEVELOPMENT OF THE THIRD-PARTY DOCTRINE

But such flexibility is accompanied by a lack of clarity that can frustrate the Court. At times, the Justices have sought greater predictability in Fourth Amendment jurisprudence.[54] Unfortunately, that approach has created bright-lines that fail to respond to the modern world. One example is the current third-party doctrine.[55]

The Court summarized that

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[56]

---

[53] The Justices are cognizant of the need to look to the forward march of investigative capabilities given evolving technologies. "[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[54] *See* Riley v. California, 134 S. Ct. 2473, 2491–92 (2014) (recognizing that police officers must have clear, workable rules created "on a categorical basis—not in an ad hoc, case-by-case fashion" (quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981))).

[55] Again, I have described the evolution of this doctrine in great detail in other work. *See* Gentithes, *supra* note 11, at 943–48. There, I noted that the doctrine first emerged in cases concerning verbal statements made to third parties that turned out to be government informants, situations where "the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications." Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (citing Lopez v. United States, 373 U.S. 427, 439 (1963); Hoffa v. United States, 385 U.S. 293, 302–03 (1966); United States v. White, 401 U.S. 745, 751–52 (1971)).

[56] United States v. Miller, 425 U.S. 435, 443 (1976).

The third-party doctrine is thus a blunt instrument. Rather than acknowledge gradations in the sensitivity of information citizens disclose to others, it provides a simple, if oft-criticized, norm: government collection of information disclosed to non-governmental third parties does not constitute a search subject to Fourth Amendment requirements.[57]

The third-party doctrine evolved largely in two influential cases from the 1970s—*Miller*[58] and *Smith v. Maryland*.[59] First, in *Miller,* government investigators obtained financial records of two accounts from a defendant's bank via an admittedly defective subpoena, including microfilm records for each account, "all checks, deposit slips, two financial statements, and three monthly statements."[60] The defendant challenged the admission of his bank records as the fruit of an unlawful search.[61] The Supreme Court held that because "[a]ll 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," there was no reasonable expectation of privacy in those records, and thus the government did not conduct a search when it collected them.[62] The defendant assumed the risk that third-party bankers would reveal his sensitive financial information to the government, tacitly consenting to such disclosures.[63]

Three years later in *Smith*, police officers warrantlessly asked a telephone company to install a pen register device in its central offices to record the numbers dialed from the home phone of a man suspected of robbing and later harassing a Baltimore woman.[64] That device "disclos[ed] only the telephone numbers that [the defendant]. . . dialed."[65] The Court held that the government's installation of that device did not constitute a search because the defendant had

---

[57] For a brief summation of critiques of the third-party doctrine, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009).

[58] 425 U.S. at 435.

[59] 442 U.S. 735 (1979).

[60] *Miller*, 425 U.S. at 438.

[61] *See id.* at 436.

[62] *Id.* at 442.

[63] *Id.* at 443. Another rationale underlying *Miller* was the fact that banks traditionally kept these records, so the government's effort to collect them was not a "novel means designed to circumvent established Fourth Amendment rights." *Id.* at 444.

[64] *Smith*, 442 U.S. at 737.

[65] *Id.* at 741.

no reasonable expectation of privacy in the numbers he dialed and thereby disclosed to a third party.[66] Telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[67] Thus, the government was not required to obtain a warrant prior to collecting such information through a pen register, because the defendant had no reasonable expectation of privacy in that information in the first place.[68]

B. LIMITS OF THE THIRD-PARTY DOCTRINE

Miller (and, to a lesser extent, *Smith*) suggests an unlimited investigative technique for government investigators in today's world. *Miller* implies that investigators can warrantlessly obtain *any* information a citizen discloses to a third-party service provider, no matter how sensitive the information is or how detailed an informational mosaic of the citizen it may paint.[69] But as expansive as the third-party doctrine seems, it always had inherent limits. Contrary to champions' arguments,[70] the third-party doctrine was

---

[66] *Id*. at 743–46 (citing *Miller*, 425 U.S. at 442–44).

[67] *Id*. at 743.

[68] *Id*. at 745–46. Justice Marshall vigorously dissented from the majority's assumption of the risk rationale in *Smith*. Marshall noted that

> [i]mplicit in the concept of assumption of risk is some notion of choice . . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.

Id. at 749–50 (Marshall, J., dissenting) (citing Lopez v. United States, 373 U.S. 427, 465–66 (Brennan, J., dissenting)).

[69] *Cf.* Gray & Citron, *supra* note 18, at 68–69; Kerr, *supra* note 18, at 313 ("Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps.").

[70] Justice Kennedy summarized this absolute view of the third-party doctrine in his dissent in *Carpenter*. 138 S. Ct. 2206, 2232 (2018) (Kennedy, J., dissenting) ("[T]he fact that information was relinquished to a third party was the entire basis for concluding that the defendants in [*Miller* and *Smith*] lack a reasonable expectation of privacy. *Miller* and *Smith* do not establish [any] kind of category-by-category balancing . . . .").

never a limitless rule that every datum provided to a third party was warrantlessly available to the government.[71]

For instance, while investigators can warrantlessly collect dialed telephone numbers,[72] they cannot collect the words spoken in the subsequent conversation, which are also provided to third parties.[73] Similarly, the government cannot warrantlessly collect medical information disclosed to third-party doctors: "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[74] Nor can investigators search a suspect's hotel room without a warrant, despite the fact that third-party housekeepers or maintenance people may have accessed the room or even moved the suspect's belongings.[75] Fourth Amendment protections also extend

---

[71] *See* United States v. Davis, 785 F.3d 498, 527–28 (11th. Cir. 2015) (Rosenbaum, J., concurring) ("Supreme Court precedent fairly may be read to suggest that the third-party doctrine must be subordinate to expectations of privacy that society has historically recognized as reasonable. Indeed, our privacy expectations in modern-day hotels and the content of our telephone conversations hearken back to historically recognized reasonable expectations of privacy."); Kerr, *supra* note 15, at 1038 ("The claim that rights in the contents of communications should be waived under the third-party doctrine does not work because the same argument could be made about telephone calls and postal letters. A person who makes a telephone call discloses the contents of the call to the phone company: the electrical signal travels by wire to the phone company and the phone company routes the call to its destination. *Katz* established that the third-party doctrine does not apply in that setting.").

[72] *See Smith*, 442 U.S. at 745–46 .

[73] *See* Transcript of Oral Argument at 51, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) ("People disclose the content of telephone calls to third parties. But we said the government can't intrude without a warrant in that situation.").

[74] *See* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001); *see also* Transcript of Oral Argument at 23, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) ("We limited it when—in *Bond* and *Ferguson* when we said police can't get your medical records without your consent, even though you've disclosed your medical records to doctors at a hospital.").

[75] *See Davis*, 785 F.3d at 527 (Rosenbaum, J., concurring) ("[T]he Supreme Court has held that '[a] hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office.' This is so, even though housekeepers and maintenance people commonly have access to hotel rooms during a guest's stay and can view and even move around a guest's belongings in order to conduct their duties. But the fact that a hotel guest has exposed his or her belongings to hotel workers does not, in and of itself, entitle the government to enter a rented hotel room and conduct a warrantless search." (quoting Hoffa v. United States, 385 U.S. 293, 301 (1966) (citing Minnesota v. Carter, 525 U.S. 83, 95–96 (1998) (Scalia, J., concurring)))); Minnesota v. Olson, 495 U.S. 91, 96–97 (1990)); *see also* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) ("Hotel guests, for example, have a reasonable expectation of privacy in their rooms. This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate

to a suspect's rental apartment, "even though his landlord has the right to conduct unannounced inspections at any time."[76]

Each of these limitations on the third-party doctrine seems to carry its own inherent logic—the prospect of government collection of phone conversations, medical data, or the contents of hotel rooms is especially unsettling in its own unique way. The Court's technique in each case was also consistent; it categorically excluded some types of data from warrantless collection, even after it had been disclosed to a third party. But much as it failed to announce a clear rationale for excepting a week's worth of CSLI from the third-party doctrine in *Carpenter*, the Court failed to supply a justification for its earlier categorical exceptions to the doctrine.

The Court might have formed a coherent sensitivity rationale for categories of data that are, at least in some amounts, excepted from the third-party doctrine. It could have noted that some information, like the contents of our conversations or the medical data our doctor collects, is simply too sensitive to be stripped of all protection immediately upon disclosure to a third party. That rationale would fit snugly with the Court's trepidation about subjecting CSLI to the third-party doctrine in any amount given its "deeply revealing nature . . . its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[77] Such a sensitivity rationale was even clear to the dissenting Justices in *Carpenter*.[78]

Yet despite the potential clarity the *Carpenter* majority could have achieved by announcing a sensitivity rationale for its categorical approach to the third-party doctrine, it demurred, apart from vaguely referencing the "unique nature" of CSLI's "intimate window" into a customer's life.[79] Why would the majority avoid clearly announcing that certain categories of information are too

---

expectation of privacy in their apartments. That expectation persists, regardless of the incursions of handymen to fix leaky faucets." (citations omitted)).

[76] O'Connor v. Ortega, 480 U.S. 709, 730 (1987) (Scalia, J., concurring) *quoted in* SCHULHOFER, *supra* note 11, at 131.

[77] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[78] *Id*. at 2262 (Gorsuch, J., dissenting) ("Today the Court suggests that *Smith* and *Miller* distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to 'extend' those decisions to particular classes of information, depending on their sensitivity." (emphasis in original)).

[79] *Id*. at 2217, 2232.

sensitive to be subject to an absolutist version of the third-party doctrine? Because that rationale faces an awkward hurdle: the obvious sensitivity of the financial information the Court ruled wholly unprotected in *Miller*. As Justice Kennedy noted in dissent in *Carpenter*, *Miller*-style financial information seems at least as sensitive as CSLI; they are of "vast scope," including "comprehensive account[s] of almost every transaction an individual makes on a daily basis" that is accessible "[w]ith just the click of a button" and "at practically no expense."[80]

As I argue in the next part, the time has come to remove that hurdle by ending *Miller*'s time and announcing that sensitivity matters. The Court can then follow the outline of *Carpenter* and analyze the sensitivity of categories of information disclosed to third parties using a formal framework capable of clear, consistent application. Below, I prescribe a two-step method for that formalization of the categorical approach to the third-party doctrine, based upon informational sensitivity.

II. THE END OF *MILLER*'S TIME

Miller has always had its opponents, even amongst the Justices who heard the case. But that opposition has been focused primarily on abolition of the third-party doctrine as a whole. These abolitionist arguments typically challenge the Court's claim that citizens "voluntarily" disclose information to third parties that provide practically necessary services, like financial institutions or telecommunications providers. In this section, I propose a more lasting critique to adjust, rather than abolish, the third-party doctrine, based upon the inherent sensitivity of some types of information that citizens relay to third parties.

A. INVOLUNTARY ASSUMPTION OF THE RISK

In his dissent in *Miller*, Justice Brennan criticized the majority's rationale that bank customers voluntarily assume that risk of third-party disclosure.[81] As Brennan noted, "[f]or all practical purposes, the disclosure by individuals or business firms of their financial

---

[80] *Id.* at 2232–33. (Kennedy, J., dissenting).

[81] United States v. Miller, 425 U.S. 435, 448–51 (1976) (Brennan, J., dissenting).

affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[82] Thus, Brennan asserted that bank customers reasonably believe that the financial information they disclose "will be utilized by the bank only for internal banking purposes," absent compulsion by legal process.[83]

The assumption of the risk rationale met similar resistance from some Justices in *Smith* three years later. There, Justice Stewart questioned whether "there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."[84] Further, Justice Marshall noted that

> Implicit in the concept of assumption of risk is some notion of choice. . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.[85]

These critiques were echoed again in *Carpenter*, but this time in the majority opinion. Chief Justice Roberts emphasized that the use of cell phones is "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern

---

[82] *Id.* at 451.

[83] *Id.* at 449.

[84] Smith v. Maryland, 442 U.S. 735, 747 (1979) (Stewart, J., dissenting).

[85] *Id.* at 749–50 (Marshall, J., dissenting) (citations omitted). In the years since *Smith*, these critiques have been repeated in the academic literature. *See, e.g.*, ABA STANDARDS, *supra* note 4, at std. 25-4.1(a) (stating that transferring information to third parties is "reasonably necessary to participate meaningfully in society"); BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 236 (2017) ("'Voluntarily' is the trick word here . . . . [I]n today's world we have little choice but to give our most intimate information to third parties all the time."); Price, *supra* note 6, at 267 ("It is . . . impossible to fully participate in modern economic life without involving a bank to execute transactions. Because this third-party interaction is unavoidable, it undermines the assumption of risk rationale."); Kerr & Nojeim, *supra* note 6 ("If you want to communicate efficiently today, your communications likely will go through your ISP's servers. The alternative means of communication either involve conveying information to other third parties, or traveling to the other communicant so you can have a personal chat. Consent in this context has little meaning.").

society."[86] Cell phones generate CSLI through "[v]irtually any activity on the phone."[87] Thus, a cell phone user does not meaningfully assume the risk of disclosure of that information to third parties, including government agents.[88]

An important distinction arises, though, in the *Carpenter* majority's use of the critique. There, the Court used the critique to suggest that the third-party doctrine should be limited, rather than to propose its abolition. Rightly so. Critiques of the assumption-of-the-risk rationale do not eliminate a kernel of truth at the third-party doctrine's core. Orin Kerr describes this as the "eyewitness rule"—the idea that there is no Fourth Amendment right preventing others from telling the government what they have seen or heard about you.[89] Critics often fail to acknowledge that when we disclose information to others—even if that disclosure is mundane and practically necessary—nothing prohibits those others from violating our trust and relaying that information again.[90] Claims that the third-party doctrine is wholly invalid because such disclosures are practically involuntary disregard that kernel of truth. Entirely overruling the doctrine is strong medicine—perhaps too strong for police investigators, or the rationale underlying this area of jurisprudence, to bear.

B. SENSITIVITY MATTERS

I prescribe a more measured adjustment to the third-party doctrine, one that would supplement the categorical approach described in the *Carpenter* majority with a clear, workable rationale. My prescription is based upon a secondary strand to Brennan's *Miller* dissent. Brennan noted the sensitivity of the information at issue, recognizing that "the totality of bank records provides a virtual current biography" of the customer.[91] In other

---

[86] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (quotation omitted).

[87] *Id.* at 2220.

[88] *Id.*

[89] Kerr, *supra* note 4.

[90] The Court showed its understanding of that idea in *Hoffa v. United States*, in which the court permitted the government to warrantlessly obtain information from a third-party witness in whom the defendant had confided. 385 U.S. 293, 302 (1966). Similarly, the ABA's proposed standards on law enforcement access to third party records highlight the resonance of the third-party rationale. *Supra* note 4.

[91] United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

words, there is something constitutionally relevant about the very nature of financial information, separate and apart from how that information was disclosed and to whom.

Informational sensitivity explains why *Miller*, though important in establishing the logic of the third-party doctrine, contains a holding about financial information that is actually a third-party-doctrine outlier.[92] Critics of the doctrine are not worried about each and every mundane data point that might be collected from a third-party, but instead about the particular sensitivity of some of the data points inevitably included in government data dragnets.[93] Some data points are particularly sensitive, and ought to enjoy constitutional protection even if disclosed to a third party. Some pieces of information are particularly disturbing to citizens when disclosed by a third party, such as the trip to the abortion clinic or the choice to worship in a community of faith.[94] When the government obtains such sensitive information from a third party, it raises heightened Fourth Amendment concerns, especially in light of the possibility that bad government actors could improperly manipulate that information.[95]

Informational sensitivity was also at the core of the *Carpenter* majority's discomfort with warrantless collection of CSLI, though it was not clearly expressed in the opinion. Over and over, the majority emphasized that "CSLI is an entirely different species of business record," one that "provides an intimate window into a

---

[92] *See* Ferguson, *supra* note 12, at 566 ("Underlying the protection of most persons, homes, papers, effects, and expectations of privacy is a concern for personal information—information that allows for self-expression, autonomy, association, religion, liberty, family, and security." (citation omitted)).

[93] *See* Priscilla J. Smith, *Much Ado About Mosaics: How Original Principles Apply to Evolving Technology in* United States v. Jones, 14 N.C. J.L. & TECH. 557, 580–81 (2013) ("The most common examples of [GPS] technology's intrusiveness involve the possibility that certain information will be obtained—information that is found on just one 'tile' in the mosaic and that can be gathered from just one trip."). Thus, there exists "a broader concern that Government spying could lead to a world in which the government needs only to run a quick search through the database to find something—just one thing—you wish it had not seen." *Id.* at 581.

[94] *See id.* at 581.

[95] *See* SLOBOGIN, *supra* note 24, at 195 ("A separate concern about event-driven data mining is that because it can cast such a wide net, it is easier to manipulate in the service of illegitimate ends. In particular, it might facilitate both harassment of disfavored groups . . . and pretextual searches for evidence of nonprofiled crimes that the government would otherwise have difficulty discovering or proving. . . .").

person's life" and is "exhaustive" and "distinct" from other information disclosed to third parties.[96]

These gestures towards the sensitivity of CSLI are vital to reshaping the third-party doctrine. Long-term location information about nearly every citizen, which can recreate our paths in the world for as long as cell phone companies preserve their records, are acutely sensitive. The *Carpenter* majority's analysis sought to balance that informational sensitivity with the kernel of truth at the third-party doctrine's core. Incorporating informational sensitivity expressly into the Court's analysis would more aptly describe the relevant considerations when government investigators begin to acquire new types of digital information in bulk.

Sensitivity matters because it shows why government collection of massive troves of some informational categories amounts to a search, while government collection of individual data points may not. If some types of information are inherently sensitive, then warrantless government collection of enough of that information can violate the Fourth Amendment under the "mosaic theory" (also known as the "quantitative theory") of the Fourth Amendment.[97]

The mosaic theory posits that citizens have reasonable expectations of privacy "in certain quantities of information and data even if [they] lack reasonable expectations of privacy in the constituent parts of [the] whole."[98] Thus, though prior jurisprudence permits the government to warrantlessly collect individual data points—say, individual pieces of your trash[99]—the mosaic theory provides that the government must obtain a warrant if it collects

---

[96] Carpenter v. United States, 138 S. Ct. 2206, 2217, 2219 (2018).

[97] *Cf.* Smith, *supra* note 93, at 560–61 (arguing that "[u]nder a ruling that relied *solely* on the mosaic theory, surveillance would invade a reasonable expectation of privacy whenever it collected individual pieces of information about a person's location" because of the sensitivity of the information (emphasis in original)).

[98] David Gray & Danielle K. Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 390 (2013). For a more detailed explanation of the origins of the mosaic theory, see Gray & Citron, *supra* note 18, at 68–69 (describing a more interwoven approach as compared to the once "theoretically and practically discrete" fields of information privacy law and Fourth Amendment jurisprudence); Kerr, *supra* note 18, at 313 (explaining the cases that gave rise to the theory).

[99] *See* California v. Greenwood, 486 U.S. 35 (1988) (holding that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home).

enough of those data points to paint a (perhaps messy) picture of your life.

The mosaic theory is open to attack on the grounds that no quantity of absolute non-searches could ever equal a search.[100] But that attack is premised upon a reading of the third-party doctrine in absolute, binary terms, such that government collection of individual data points is either 100% or 0% of a search. That hard rule has long been eroded around its edges, and the *Carpenter* majority continued that erosion.[101] The Court's jurisprudence concerning some types of information, such as the contents of conversations or diagnostic medical testing, suggests an evolution in the doctrine.[102] Though the foundational insight that disclosure to others is constitutionally relevant remains, the doctrine has progressed from a hard rule to a flexible standard. The Court should further this progression by explicitly examining the sensitivity of the information at issue in third-party doctrine cases.

There is a continuum of sensitivity upon which data falls, which in turn dictates varying expectations of privacy in that data even after it has been disclosed to a third party. On one end is pure meta-data with no inherent meaning, such as the dialed phone numbers in *Smith*. On the other end are extremely sensitive data-points, such as medical information in the control of health care professionals. In the middle are a number of categories that carry some inherent magnitude of sensitivity, data that inherently conveys some miniscule amount of meaning. Citizens harbor some miniscule reasonable expectation of privacy in that data, such that an aggregation of those miniscule integers can amount to a search for which the government must first obtain a warrant, even if a citizen disclosed that data to a third party.[103]

---

[100] For a discussion of this problem, and one possible solution to it, see Gentithes, *supra* note 11, at 958–60. Unlike my position in that Article, my argument here is that individual citizens rightly retain a miniscule expectation of privacy in location data points, such that a sufficient accumulation of those greater-than-zero invasions of privacy amounts to a single search.

[101] *See supra* notes 77–78 and accompanying text.

[102] *See supra* notes 72–76 and accompanying text.

[103] Even Professor Orin Kerr, a long-time defender of the third-party doctrine, has acknowledged that Fourth Amendment cases involving emerging data-collection technologies should be controlled by the type of data at issue, rather than how the government collected it. According to Kerr, "[i]n areas of new technology, the details of how the information is collected can be contingent and unstable. Focusing a rule on the kind of information that is

Other scholars have attempted to categorize information on a sliding scale. For instance, Andrew Guthrie Ferguson has proposed a continuum to distinguish between protected and unprotected data emanating from digital "smart" devices. According to Ferguson:

> The analysis would necessarily work along a continuum, with little to no protection for information freely shared with others (commenting through a public Twitter account), to more protection for users who controlled locational data access, restricted data sharing, and used encrypted services, to absolute protection for people technologically savvy enough to use key encryption or establish contractual arrangements to secure data.[104]

Michael W. Price has also argued that the binary classification created by the third-party doctrine is problematic in the modern world. As he puts it, "sharing digital data is not an all-or-nothing endeavor; it is more like a sliding scale that users may control (although not always with success)."[105]

The most nuanced of these sliding scale efforts was the American Bar Association's 2012 Proposed Standards for Law Enforcement Access to Third Party Records, which claims that courts and legislatures should consider the "privacy" of information that the government collects.[106] The ABA's proposal labeled all types of information as either highly private, moderately private, minimally private, or not private.[107] Courts could implement this sliding scale based upon consideration of whether:

> (a) the initial transfer of such information to an institutional third party is reasonably necessary to

---

collected, rather than the details of how it is collected, is often a more stable and consistent approach." Orin Kerr, *The Best Way to Rule for Carpenter (Or, How to Expand Fourth Amendment Protections Without Making a Mess)*, LAWFARE (Dec. 29, 2017, 6:03 AM), https://lawfareblog.com/best-way-rule-carpenter-or-how-expand-fourth-amendment-protections-without-making-mess.

104 Ferguson, *supra* note 12, at 621–22.

105 Price, *supra* note 6, at 268.

106 ABA STANDARDS, *supra* note 4, at std. 25-4.1.

107 *Id*.

> participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;
> (b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;
> (c) such information is accessible to and accessed by non-government persons outside the institutional third party; and
> (d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.[108]

My informational sensitivity view takes a new perspective on such efforts, directly responding to the *Carpenter* Court's expressed interest in a categorical third-party doctrine by establishing a continuum of informational sensitivity. Unlike the ABA's emphasis upon the "personal" and potentially stigmatizing nature of information,[109] my view emphasizes the substantive meaning that information conveys on its face, irrespective of the stigma that meaning may carry.[110] By emphasizing whether investigators can instantaneously draw conclusions about citizens based upon a mere glance at the information at issue, my view focuses on objective characteristics of the information, rather than the stigma associated with informational categories that judges either would have to assume or would have to learn through significant empirical research.[111]

I suggest that when determining placement on my proposed continuum of informational sensitivity, the Court look to other developments in its own jurisprudence that suggest special

---

[108] *Id.*

[109] *See id.*

[110] *See infra* Part II.C.

[111] As noted earlier, such explicitly empirical approaches to the third-party doctrine appear difficult, if not impossible, to operationalize. *See supra* note 47.

constitutional protection for that category of information.[112] As detailed in the next subsection, my informational sensitivity continuum uses a two-step framework to expressly incorporate the mosaic theory of the Fourth Amendment only for information that has some inherent sensitivity at the first step.[113] While the ABA's proposal leaves unanswered whether collection of information labeled "not private" could ever amount to a search, my proposal expressly excludes collection of non-sensitive information from classification as a search, no matter how much of that information the government collected.[114]

This view is consistent with my earlier work on the mosaic theory and constitutional tranquility. I have argued that government data dragnets that collect completely innocuous, non-sensitive information about all citizens can still be a search.[115] Citizens share an interest in constitutional tranquility, an under-theorized concept[116] grounded in the Constitution's text[117] and in Justice Brandeis's conception of the primary aim of the Fourth Amendment

---

[112] *See infra* Part II.C.1. In contrast, the ABA's approach looks more to legislative sources of law to determine the privacy of information. *See* ABA STANDARDS, *supra* note 4, at std. 25-4.1.

[113] *See infra* Part II.C.2.

[114] *See id.*

[115] Gentithes, *supra* note 11, at 961 ("[E]ach government action is an infringement upon the tranquility implicit in the Fourth Amendment, and a sufficient aggregation of such infringement is a search.").

[116] *See id.* at 961

> [C]onstitutional tranquility . . . implies a level of peace and quiet in our daily affairs, and suggests that the default position of government is one of inaction, not aggressive intrusion into citizens' lives . . . . It makes no difference if the government effort is unknown to citizens; the tranquil foundation of life in a free republic is disrupted by the activity itself, not by its effect upon citizens' consciousness. The disruption impairs constitutional tranquility.

[117] Tranquility is one of the overarching purposes of the Constitution, given expression in its preamble, promising to "insure domestic Tranquility." U.S. CONST. pmbl. *See also* Gentithes, *supra* note 11, at 962

> Constitutional tranquility is reflected in the text beyond the Fourth Amendment . . . . The Third Amendment's prohibition against the unconsented peacetime quartering of soldiers protects another aspect of privacy from governmental intrusion. Even more, to some extent, the Fifth Amendment too reflects the Constitution's concern for the right of each individual to a private enclave where he may lead a private life. These textual assurances depend on a baseline level of undisturbed domestic tranquility.

Quotations and citations omitted.

as protecting "the right to be let alone."[118] That shared tranquility interest can be undermined by the collection of data points in which citizens have absolutely no reasonable expectation of privacy—such as the phone numbers they dial.[119] The collection of each data point is a "greater-than-zero intrusion" upon our shared tranquility interests, and those intrusions can be aggregated to the point that a data dragnet constitutes a search—such as where a dragnet captures data about practically everyone engaged in a ubiquitous activity like dialing a phone.[120]

In contrast, my argument here is that individual citizens rightly retain a miniscule expectation of privacy in sensitive data points. Thus, each collection of those sensitive data points is a greater-than-zero invasion of privacy. And a sufficient accumulation of those greater-than-zero invasions of privacy amounts to a single search.

My view also answers one of Orin Kerr's primary concerns with mosaic theory—that citizens cannot maintain an expectation of privacy in data amassed at discrete intervals, such as several non-consecutive weeks of banking information spread over several years.[121] So long as there is some minimal expectation of privacy in each individual datum the government collects, whether it collected the data points over a consecutive period is irrelevant. The amalgamation of those individual data points, each of which carries some magnitude of inherent sensitivity, can amount to a positive integer, and in turn can amount to a single Fourth Amendment search.

My approach is an important supplement to current practice signaled by the *Carpenter* majority. Rather than preserving the myth that all information citizens disclose to third parties is stripped entirely of constitutional protection—a myth the Court has long undermined,[122] and which it all but buried in *Carpenter*[123]—my approach disposes of *Miller*'s false dichotomy and replaces it with a continuum that explains the Justices' discomfort in many recent

---

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

119 Gentithes, *supra* note 11, at 959.

120 *Id.* at 963.

121 *See* Kerr, *supra* note 18, at 334.

122 *See supra* Part I.B.

123 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

third-party-doctrine cases. Sensitivity provides the missing rationale around which a majority of the Justices can coalesce when expressing their discomfort with an absolutist third-party doctrine. It explains how the old third-party-doctrine approach may be "ill suited to the digital age,"[124] but a refined doctrine can still retain salience in the many cases where the government obtains only a few data points about relatively non-sensitive information. And as I explain below, it is an approach the Court can apply over time to emerging technologies as part of a good-faith, workable effort to set proper limits for the third-party doctrine.

C. TWO-STEP TEST FOR INFORMATIONAL SENSITIVITY

My approach will require the Court, in cases where the government obtained large amounts of data from a third party, to undertake a two-step test to determine whether a warrant was required. As noted above, it is thus a more formalized, and more judicially manageable, approach to categorizing information than previous efforts at determining the Fourth Amendment protection based upon a sliding scale of privacy.[125]

In the first step, the Court should determine the sensitivity of that information, placing it on a sensitivity continuum rather than a false dichotomy between disclosed and undisclosed information. This approach will allow the *Carpenter* majority's categorical approach to the third-party doctrine to evolve in a straightforward, workable fashion—and away from a hard rule that fails, as the Court itself has acknowledged, for some categories of information.[126] Several sources can determine informational sensitivity: the Court's own treatment of the category of information at issue in other decisions that touch upon it, in the criminal context or elsewhere; the substantive meaning that the information conveys on its face; and the relative voluntariness of the disclosure of that information in contemporary society.

In the second step, the Court should decide whether the government has collected enough sensitive information to create an informational mosaic of the citizen, thereby conducting a search.

---

[124] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[125] *See supra* Part II.B.

[126] *See supra* notes 72–76 and accompanying text.

Citizens have a small but cognizable expectation of privacy in many data points that a third party collects, depending upon the data's relative sensitivity. Though government collection of one or even several intermediately sensitive data points may not raise constitutional concern, if the government collects enough of them, it creates such a detailed picture of the citizen's life that it has conducted a search for which it must usually obtain a warrant.

1. Step One: Determining Sensitivity

The first step will require the Court to place the information at issue on a continuum of sensitivity. To make that determination, the Court can initially consider other developments in its own jurisprudence that shed light upon the question. Where the Court's decisions in other areas have suggested that such information is of unique constitutional concern, the Court should place that category of information near the sensitive end of the continuum. In the following subsection, I discuss two examples where the Court has indicated such unique constitutional concerns—financial transactions like those at issue in *Miller* and reading record concerns that it has raised in other contexts.[127] The Court can look for such developments when deciding whether information is sensitive enough to warrant some Fourth Amendment protection under my proposal.

When determining sensitivity, the Court can also consider the level of substantive meaning inherent in the information at issue. For instance, while raw data like telephone numbers conveys relatively little substantive detail, a history of financial transactions, which might indicate the products, costs, and vendors in thousands of commercial interactions, conveys far more meaning. Information with such an inherent vector of substantive meaning is more sensitive and more likely to fall on the sensitive end of the continuum.

Information that conveys greater facial meaning is more sensitive, and hence more constitutionally protected under my theory, because even local authorities with limited data-aggregation capabilities can readily discern the intimate details of a suspect's life after collecting just a few such data points. My position offers

---

[127] *See infra* Part II.D.

heightened protection for such facially sensitive data. That heightened protection ensures that in local investigations of most criminal offenses, government agents will not be able to readily assemble intimate portraits of suspects without a warrant.

The Court's sensitivity determinations can also account for the relative voluntariness of the disclosure. As outlined above, one refrain in critiques of the third-party doctrine is that citizens cannot assume the risk of third-party disclosures where they have no choice but to utilize third-party services to survive in the modern world.[128] Though that critique does not defeat the third-party doctrine's insight that disclosure is still constitutionally relevant, it is not an irrelevant consideration in Fourth Amendment analysis. As the Court intimated in *Carpenter*,[129] the relative voluntariness of a disclosure can play a meaningful role in informing the Court's sensitivity judgments during the first step of my test.

Though the Court will need to rely upon its own value judgments to some extent to determine the sensitivity of information, it can also rely upon the arguments fleshed out by parties and amici to fully comprehend technological advances and the ubiquity of data disclosures. Interested parties can explain the frequency, depth, and detail of citizens' disclosures of a particular category of information to third-party service providers. For instance, the arguments might show, in the case of *Miller*-style financial information, how detailed and meaningful bank records of consumer transactions are in today's society.[130]

Even with these sources in hand, the Court will likely find bright lines elusive. But the lack of bright lines is acceptable for this aspect of Fourth Amendment jurisprudence. To be clear, I only suggest that the Court consider informational sensitivity when the government has collected information from third parties, and only then to determine whether warrantless collection is permissible under the third-party doctrine. I do not contend here that

---

[128] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting); ABA STANDARDS, *supra* note 4, at std. 25-4.1(a); FRIEDMAN, *supra* note 85, at 237; Price, *supra* note 6, at 267; Kerr & Nojeim, *supra* note 6.

[129] *See* Carpenter v. United States, 138 S. Ct. 2206, 2208 (2018) (discussing the voluntariness of cell phone location data disclosure). My position aligns with the *Carpenter* majority's approach, which included the suggestion that the third-party doctrine did not fully apply to CSLI because customers did not meaningfully make voluntary disclosures of it. *Id.*

[130] *See infra* notes 158–159 and accompanying text.

informational sensitivity is a vital component in the Court's broader Fourth Amendment jurisprudence.

One might object that informational sensitivity is far too indeterminate to form the basis of a constitutional rule.[131] If Justices must rely, even in part, upon their own values to determine the sensitivity of, and hence level of Fourth Amendment protection for, categories of disclosed information, jurisprudence in this area will be reduced to nine people's rudderless assumptions about technology and consumer habits. But while informational sensitivity is a messy continuum, fleshing out that continuum, at least on a provisional basis while new technology emerges,[132] is worthwhile. A genuine effort to craft such a tentative rule is vital to the public's perception that the Court is upholding the Fourth Amendment's protections afforded to all of "the people," not just the criminal defendants in the Court's headline third-party-doctrine cases.[133] That process, though messy, will demonstrate the Court's good-faith, nuanced effort to protect citizens' widespread disclosures of data to third-party service providers in an appropriate way.

2. Step Two: Sensitivity and Mosaics

Where the Court determines that the information collected had some sensitivity, it should proceed to the second step of the test. Again, the second step is unnecessary if the information is not sensitive. Pure metadata like telephone numbers dialed may not be sensitive, and the government may warrantlessly collect it in bulk without violating expectations of privacy.[134] But if the information is sensitive, the Court should determine whether the government has collected enough of it to create an informational mosaic of the citizen. Depending upon where the information falls on the sensitivity continuum and how much the government has obtained, the Court can then determine whether the government's conduct

---

[131] *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting) (commenting that he "do[es] not know and the court does not say" what sensitive means).

[132] *See infra* Part IV. The Court can adjust course with a freer hand than in most areas of jurisprudence in the future as both citizens and service providers offer new uses for and perspectives upon different types of data.

[133] *See* U.S. CONST., amend. IV; *see also supra* notes 33–35 and accompanying text.

[134] *But see* Gentithes, *supra* note 11, at 960–66 (presenting an alternative theory of why the limitless collection of pure metadata may nonetheless violate citizens' rights to constitutional tranquility).

amounted to a search under the mosaic theory of the Fourth Amendment.[135]

Importantly, the government can warrantlessly collect one or even several data points of a person's most sensitive information. Aside from a few categories of extremely sensitive data, such as the medical records the Court has already excepted from the third-party doctrine,[136] the government may still warrantlessly collect most individual data points. All the Court needs to determine at this step is whether the government has assembled enough sensitive data points to paint a detailed picture of a citizen's life, and therefore conducted a search for which a warrant is required in spite of the third-party doctrine.

This position dovetails with the *Carpenter* majority's limited holding, which applies only to the collection of at least seven days' of CSLI and not to "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)."[137] That distinction's logic draws upon the relative sensitivity of CSLI—more so than *Smith*'s telephone metadata, but less than completely excluded third-party information like medical diagnostic test results.[138] Thus, collection of a few data points of CSLI, or of single data points of multiple citizens in one area at a specific time, might be permissible under the second step of my proposed analysis.

Police officers and government investigators may find it difficult to determine the threshold for collection of sensitive information ex ante.[139] That difficulty is acceptable. Again, government investigators need not hesitate to collect individual data points of

---

[135] *See supra* Part II.B; Gray & Citron, *supra* note 98, at 390 (describing the mosaic theory of Fourth Amendment privacy and the primary objections to it); Gray & Citron, *supra* note 18, at 68–69 (discussing the practical implementation of recognizing citizens' "right to expect that certain quantities of information about them will remain private"); Kerr, *supra* note 18, at 313 (noting that five justices of the Supreme Court appear to endorse "some form" of the mosaic theory).

[136] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001); *see also* Transcript of Oral Argument at 23, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) ("We limited it when—in *Bond* and *Ferguson* when we said police can't get your medical records without your consent, even though you've disclosed your medical records to doctors at a hospital.").

[137] *Carpenter*, 138 S. Ct. at 2220 (describing the Court's decision as "a narrow one").

[138] *See id.* at 2216–17 (distinguishing *Smith* by the detail and comprehensiveness of the information collected).

[139] *See* FRIEDMAN, *supra* note 85, at 229.

almost all categories of data.[140] It is only when investigators seek extensive third-party records of sensitive information, as part of their own extended investigations—not as part of the rapid-fire, life-and-death decisions officers often must make in the field—that the investigators must first obtain judicial approval.[141] Giving government agents some hesitation in those scenarios is not a bug, but a desirable feature. The extra investigation and paperwork that might be involved if officers, uncertain of the level of protection that a category of information might receive upon later judicial review, decide to seek an unnecessary warrant in order to obtain troves of sensitive data about citizens is a fair price to pay for greater society's privacy.[142]

D. SENSITIVITY IN PRACTICE

In this subsection, I demonstrate how the Court might apply the two-step sensitivity test I propose in two examples. First, I consider the financial information at issue in *Miller*, concluding that the Court incorrectly allowed the government unlimited warrantless access to that information, even if that decision validly established the third-party doctrine's intellectual underpinnings. I then apply my test to a hypothetical case concerning emerging issues for digital reading records in libraries.

1. Financial Information

Though *Miller* remains a vital component of the third-party doctrine's origins, the particular holding it reached concerning warrantless access to unlimited amounts of financial information is flawed. The *Miller* court permitted the government to obtain "all records"—including checks, deposit slips, financial statements, and monthly statements—pertaining to multiple accounts the defendant held at two banks during a four-month period.[143] Under

---

[140] *See Carpenter*, 138 S. Ct. at 2223 (noting that information gathered by third parties is still entitled to Fourth Amendment protections).

[141] *See supra* note 4 and accompanying text.

[142] "To the extent law enforcement wants greater clarity in any given case, there is an easy answer: get a warrant. In many of the cases in which courts have waved a green flag at the police after the fact, a warrant would have been utterly obtainable . . . . If the government can get a warrant in close cases, it should." FRIEDMAN, *supra* note 85, at 229.

[143] 425 U.S. 435, 437–38, 443 (1976).

my two-step test for the informational sensitivity of government records, that holding is dubious.

Under the first step, such financial information is highly sensitive. Several other decisions from the Court suggest that financial information is a constitutionally sensitive category. For instance, in its recent opinion in *Riley v. California*,[144] the Court acknowledged that "certain types of data are . . . qualitatively different."[145] It started by noting that internet search histories and detailed records of a person's public and private locations "could reveal an individual's private interests or concerns,"[146] adding that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[147] The Court specifically acknowledged that limitless collection of financial data stored in a digital device might raise Fourth Amendment concerns.[148] According to the Court, "[t]he fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years."[149] The Court thus recognized that financial information is sensitive enough to garner some Fourth Amendment protection.

Similarly, the Court's First Amendment jurisprudence suggests that financial information is particularly sensitive. In the landmark *Buckley v. Valeo* decision, the Court ruled that spending money to influence elections is a form of constitutionally-protected free speech.[150] According to the Court, "virtually every means of communicating ideas in . . . mass society," at least since 1976, "requires the expenditure of money."[151] The Court thus "equated money with speech and hence concluded that restrictions on spending could harm speech rights severely."[152] Applying the logic

---

[144] 134 S. Ct. 2473, 2477 (2014) (holding that police officers cannot warrantlessly search digital information on a cell phone seized incident to arrest).

[145] *Id*. at 2490.

[146] *Id*.

[147] *Id*. at 2489. Thus, in the digital age, people commonly carry "a cache of sensitive personal information" in their pockets—their cell phones. *Id*. at 2490.

[148] *See id*. at 2485.

[149] *Id*. at 2493.

[150] *See* 424 U.S. 1, 16–20 (1976).

[151] *Id*. at 19.

[152] Jessica A. Levinson, *The Original Sin of Campaign Finance Law: Why Buckley v. Valeo is Wrong*, 47 U. RICH. L. REV. 881, 933 (2012). For a summary of the Court's jurisprudence

of *Buckley*,[153] some financial transactions likely to be captured through a *Miller*-style subpoena are equivalent to protected First Amendment activity.[154] Though political donations are typically reported to the Federal Election Commission,[155] the Court's longstanding concern about government regulation of the free flow of financial transactions equated with speech highlights the special sensitivity of data about those transactions. The government simply cannot examine all the spending habits of citizens without eventually examining the contents of communications—that is, without examining money that has been spent to advance speech.[156]

The Court's holdings in *Riley* and *Buckley* suggest that financial information collected by the government should receive some Fourth Amendment protection. That suggestion is supported by the substantive meaning financial information conveys on its face. The full records of a bank customer's accounts convey something substantive to the reader. They may reveal sensitive details about the commercial interactions the bank customer has with political parties, medical professionals, paramours, or therapists. As the American Bar Association has noted, "[h]ow much we spend, where we spend it, when we spend it, and on what are paradigm examples of intimate information."[157]

The substantive content of information maintained by financial institutions has also increased over time. At the time of *Miller*, financial institutions' records included deposit slips and cancelled

---

equating money and speech, at least in the political arena, see *id.* at 890–904 and Jed Rubenfeld, *The First Amendment's Purpose,* 53 STAN. L. REV. 767, 801–07 (2001).

153 424 U.S. at 18–19.

154 *Cf.* Slobogin, *supra* note 5, at 2 ("The capacity of computers to access, store, and analyze data has made mountains of personal information—ranging from phone and email logs to credit card and bank transactions—available to government officials at virtually the touch of a button.").

155 *See* Levinson, *supra* note 152, at 891. It is worth noting, though, that speakers may keep secret their other efforts to fund the communication of ideas.

156 *See* Price, *supra* note 6, at 299 ("[I]f the Court continues to equate spending money with speech, then the rationale in *Miller* loses much of its force.").

157 ABA STANDARDS, *supra* note 4, at std. 25-4.1(b) cmt; *see also id.* ("Financial transaction records are quite personal. They do not alone indicate precisely what was purchased, but in the aggregate they provide a virtual current biography of our lives. Every time a credit card is swiped, the provider knows where the customer is located and quite a lot about what he or she is doing. The provider will not know that the good purchased was Mein Kampf, but it will know that at 10:42 a.m. this person purchased $13.49 of goods at the Borders book store in Exton, PA, and that fifteen minutes earlier he spent $7.36 at Starbucks down the street.").

checks that captured a small snapshot of a customer's financial transactions not undertaken in cash. Today's consumers use a wider variety of non-cash payment options far more frequently, generating more detailed third-party records of more financial transactions.[158] With each swipe of a credit or debit card, customers provide third parties with detailed data about their actions, locations, and preferences.[159] The financial data third parties collect today is far more sensitive than it was when *Miller* was decided, justifying a re-evaluation of government efforts to obtain it without a warrant.

Lastly, as several Justices noted in *Miller* itself, disclosure of financial information to banking institutions is all but required to exercise agency in modern society.[160] The practically compulsory nature of providing that information should also inform the Court's judgement as to financial data's relative sensitivity for third-party doctrine purposes.

Financial information of the sort at issue in *Miller* fits in the middle of the sensitivity continuum, which should lead the Court to advance to the second step of my proposed test: determining whether the government collected enough sensitive information to create an informational mosaic of the defendant citizen. The amount

---

[158] *See, e.g.*, U.S. FEDERAL RESERVE, THE FEDERAL RESERVE PAYMENTS STUDY 2016 at 2, https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf ("U.S. noncash payments, including debit card, credit card, ACH, and check payments, are estimated to have totaled over 144 billion with a value of almost $178 trillion in 2015, up almost 21 billion payments or about $17 trillion since 2012 . . . . Total noncash payments increased at an annual rate of 5.3 percent by number of 3.4 percent by value from 2012 to 2015."); CASH PRODUCT OFFICE FEDERAL RESERVE SYSTEM, THE STATE OF CASH: PRELIMINARY FINDINGS FROM THE 2015 DIARY OF CONSUMER PAYMENT CHOICE, Nov. 2016, https://www.frbsf.org/cash/publications/fed-notes/2016/november/state-of-cash-2015-diary-consumer-payment-choice ("Cash is facing competition from other payment instruments. In 2015, 32 percent of consumer transactions were made with cash, compared with 40 percent in 2012. Growing consumer comfort with payment cards and the growth of online commerce, among other factors, contribute to this trend."); TSYS, 2016 U.S. CONSUMER PAYMENT STUDY 6, https://www.tsys.com/assets/TSYS/downloads/rs_2016-us-consumer-payment-study.pdf (presenting findings from a study of 1,000 consumers and concluding that when consumers were asked for their preferred method of payment, 40% responded credit, 35% responded debit, and only 11% responded cash).

[159] *See supra* note 157.

[160] *See* United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." (quotation omitted)).

of sensitive financial information *Miller* addressed would paint just such a mosaic. Several months of financial information portrays an extremely clear picture of a citizen's most private preferences, opinions, locations, and habits. The government's collection of four months of the *Miller* defendant's account information at two banks provided detailed insights into his life. Even if the government collected individual data points from those accounts without running afoul of the Fourth Amendment, the insights collected would have been far more than any reasonable citizen should expect the government to collect warrantlessly.[161] Though *Miller* remains an important milestone in the development of the third-party doctrine, it's time as the final word on bulk collection of financial information should end.

2. Library E-Book Records

As an additional example of how the Court might implement the sensitivity continuum in a third-party-doctrine case, consider a detective's effort to obtain records of a college senior's e-book check-out history at the university library. Libraries often have detailed privacy policies, and forty-eight states and the District of Columbia maintain laws protecting library records from disclosure.[162] But third-party service providers like Amazon facilitate library borrowing on their e-readers, allowing those third parties to collect detailed reading records for later marketing use.[163] Could a detective working in a state with a restrictive library record statute

---

[161] *See* ABA STANDARDS, *supra* note 4, at std. 25-4.1(a) cmt. ("[A]n individual bank transaction may tell relatively little about a person, but records over a significant period may form a 'virtual current biography' of an individual." (quoting Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974))).

[162] BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J.L. & TECH. 1, 25 (2013) (noting that the state statutes vary, and some "allow disclosure of library records only subject to a warrant or similar process"); *see also* Kathryn Martin, Note, *The USA Patriot Act's Application to Library Patron Records*, 29 J. LEGIS. 283, 289 (2013) (collecting state statutes). Ard argues that while "librarians have built an administrative and technical architecture that is highly protective of patrons' privacy" and has "proven capable of dealing with many threats to privacy in the pre-networked world," that regime is inadequate in the digital age. Ard, *supra*, at28.

[163] *See* Ard, *supra* note 162, at 28–32 (describing a common e-book lending arrangement between Amazon and public libraries); *see also id.* at 16 ("These third parties collect sensitive user information even though they are neither integrated into our trusted institutions nor bound by the same confidentiality obligations as the institutions themselves.").

rely upon the third-party doctrine to warrantlessly obtain troves of Amazon's records?[164]

Starting with the first step of my proposed test, such reading records are moderately sensitive. As in the case of financial information, Supreme Court jurisprudence in other constitutional areas suggests that reading habits warrant constitutional protection.[165] In *Lamont v. Postmaster General of the United States*, the Court found unconstitutional a law requiring the Postmaster General to detain mail the Secretary of the Treasury identified as communist propaganda, then to maintain a list of those who requested that such mail be delivered.[166] Detaining mail would almost certainly deter free speech, "especially as respects those who have sensitive positions."[167] Citizens would feel inhibited to join a list of those who have requested literature deemed "communist political propaganda," which would undermine robust First Amendment debate.[168]

Similarly, in *United States v. Rumely*, the Court noted the constitutional sensitivity of reading records.[169] There, it considered contempt charges against a publisher who refused to reveal a list of the buyers of his "political[ly] tendentious" books.[170] The Court asserted that allowing Congress "to inquire into all efforts of private individuals to influence public opinion through books and periodicals . . . raises doubts of constitutionality in view of the prohibition of the First Amendment."[171] Justice Douglas's concurring opinion likewise maintained that "[o]nce the government

---

[164] Though some scholars have argued that the First Amendment should protect a reader's right to anonymity, "there has not yet been a case where a litigant has successfully made this argument to protect digital reader records under the First Amendment." Margot Kaminski, *Reading Over Your Shoulder: Social Readers and Privacy*, 2 WAKE FOREST L. REV. ONLINE 13, 26 (2012).

[165] *See* Ard, *supra* note 162, at 8.

[166] 381 U.S. 301, 302–03 (1965).

[167] *Id.* at 307.

[168] *Id.* In a forceful concurring opinion, Justice Brennan maintained that "[t]he dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers." *Id.* at 308 (Brennan, J., concurring).

[169] 345 U.S. 41 (1953).

[170] *Id.* at 42.

[171] *Id.* at 46. Ultimately, the Court sidestepped this constitutional issue, however. *See id.* at 46–47 ("[Prior law] strongly counsel[s] abstention from adjudication unless no choice is left. Choice is left.").

can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears."[172] These cases illustrate the Court's concern with the sensitivity of reading histories like those third-party e-reader services maintain about library patrons.

Library reading histories also convey significant substantive meaning, making them more sensitive.[173] The titles included in those histories may suggest a citizens' interest in iconoclastic political movements, minority religious groups, rare medical conditions, or even controversial theories of constitutional interpretation.[174] Where a citizen uses a library to conduct academic research, the resulting library records "are quite sensitive because they portray the user's questions and interests in vivid detail."[175] The inherent meaning in library reading records suggests that they be placed on the moderately sensitive side of the continuum I propose.

Because the use of third-party services to obtain reading materials remains somewhat voluntary, the relative sensitivity of reading histories may be tempered. This activity is not so ubiquitous as to become practically required to exercise agency in today's world. Though this fact does not wholly discount the sensitive nature of such records, it should be reflected in its placement on the sensitivity continuum. Additionally, the sensitivity of reading records may be relatively lower than that of financial information because the meaning reading records conveys is open to more varied interpretations. McCarthy-era searches of library records "produced little or no useful material, and government agents had an alarming tendency to misuse the information."[176]

---

[172] *Id*. at 57 (Douglas, J., concurring). At that point, "the spectre of a government agent will look over the shoulder of everyone who reads." *Id*.

[173] *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 436 (2008) ("Intellectual records—such as lists of Web sites visited, books owned, or terms entered into a search engine—are in a very real sense a partial transcript of a human mind.").

[174] *Cf. id*. at 389 ("The information created by [electronic technologies] includes not only our preferences in toothpaste, but our taste in politics, literature, religion, and sex.").

[175] *See* Ard, *supra* note 162, at 13.

[176] *See* Martin, *supra* note 162, at 288–89 (citations omitted); Ulrika Ekman Ault, Note, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532, 1534 (1990) (stating that the FBI was never able to justify its Library Awareness Program with any concrete evidence of its usefulness); *see also* RONALD KESSLER, THE BUREAU: THE SECRET HISTORY OF THE F.B.I. 225 (2002) ("In the end, the program

The above analysis suggests that reading records are moderately sensitive. Thus, the judge in our hypothetical case should proceed to the second step of my test and determine whether the government collected enough of that data to create an informational mosaic of the citizen, thereby conducting a search. The collection of relatively low numbers of reading records—perhaps even as low as the four-month threshold at issue in *Miller*—might not trigger the warrant requirement. But collection of four years of e-book reading records, as in this example, certainly would. The government should be required to obtain a warrant before obtaining such voluminous records from a third party.

III. THE PROVISIONAL THIRD-PARTY DOCTRINE

In the prior Part, I recommended overturning *Miller*'s expansive holding permitting unlimited warrantless collection of financial information from third parties.[177] Students of jurisprudence and legal philosophy might object that overruling the holding in *Miller* would work unacceptable violence upon well-established principles of stare decisis.[178] Such objections resonate strongly with well-meaning law enforcement personnel who must employ Fourth Amendment doctrine in their daily lives. Officers crave rulings like *Miller*—stable, clear, bright lines that are easy to implement in the field.[179] Those desires are justified given the split-second decisions that police work often encompasses. And stare decisis exists in part to let interested parties like police officers rest assured that constitutional jurisprudence will remain stable over time.[180]

---

produced very little useful information."); FRANK J. DOWNER, THE AGE OF SURVEILLANCE: THE AIMS AND METHODS OF AMERICA'S POLITICAL INTELLIGENCE SYSTEM 357 (1981).

[177] *See supra* Part II.D.*1*.

[178] I have made several arguments in favor of stare decisis on a variety of practical and philosophical bases. *See generally* Michael Gentithes, *In Defense of Stare Decisis*, 45 WILLAMETTE L. REV. 799 (2009); Michael Gentithes, *Precedent, Humility, and Justice*, 18 TEX. WESLEYAN L. REV. 835 (2012) [hereinafter Gentithes, *Precedent*].

[179] *See* Riley v. California, 134 S. Ct. 2473, 2491–92 (2014) ("[I]f police are to have workable rules, the balancing of the competing interests . . . must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers."(quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981))).

[180] Citizens' reliance interests and the practical workability of rules are primary considerations in the Court's discussion of the stare decisis principle. *See* Planned Parenthood of Southwestern Pennsylvania v. Casey, 505 U.S. 833, 854–55 (1992). Even critics of the doctrine acknowledge the importance of such reliance interests. Antonin Scalia argued that

But stare decisis should be less rigid when the Court considers new applications of the third-party doctrine. Such cases determine the constitutionality of new law enforcement techniques to gather information about suspects over an extended timeline. These techniques were often unimaginable just years earlier, let alone across the four-decade history of the doctrine.[181] Notions of privacy are necessarily contingent upon the changing landscape of technology and common practice in society. And broader society's interests are at stake when the Court determines whether the government can warrantlessly collect data in the modern, networked world. Faced with those challenges, the Court's third-party doctrine decisions should be viewed as a series of provisional prescriptions, temporarily determining whether to pause the advance of government information-gathering capabilities. Those rulings are inherently less permanent, and stare decisis should not apply to them with full force.

I do not claim, as a descriptive matter, that the Court has treated its rulings on new government information-gathering techniques as provisional.[182] Instead, the Court's steadfast dedication to third-party precedents like *Miller* has, until recently, precluded necessary adjustments to the doctrine. Decisions about new government information-gathering techniques ought to be treated as provisional to ensure that the Fourth Amendment continues to protect the privacy and tranquility of American society.[183]

Stare decisis does not simply protect reliance for reliance's sake. In part, stare decisis is an acknowledgement that for some questions, settlement is more important than accuracy.[184] For

---

"[t]he whole function of the doctrine is to make us say that what is false under proper analysis must nonetheless be held to be true, all in the interest of stability." Antonin Scalia, *Response*, *in* A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 40–41 (Amy Gutmann ed., 1997).

[181] The sheer scope of government data mining is one example. "Today the federal government alone probably operates more than 200 data-mining programs, at least 120 of which involve efforts to obtain personal information such as credit reports and credit card transaction records." SLOBOGIN, *supra* note 24, at 192.

[182] If it did, the Justices who recently questioned the constitutionality of warrantless collection of locational data could have easily coalesced around a reimagined third-party doctrine. *See* United States v. Jones, 565 U.S. 400, 413–31 (2012) (Alito, J., concurring).

[183] For a discussion of the unique public orientation of the Fourth Amendment, see *supra* note 11 and accompanying text.

[184] *See* David A. Stauss, *Common Law, Common Ground, and Jefferson's Principle*, 112 YALE L. J. 1717, 1725 (2003) ("A legal provision can settle things, and sometimes—when it is

instance, while it is not inherently clear that driving on the right side of the road is normatively superior to driving on the left, it is clear that uniform settlement of the question is far superior to ambiguity or inconsistency, which may cause more head-on collisions on the nation's highways. In other contexts within constitutional criminal procedure, clear settlement of a constitutional question is vital to ensure that officers can operationalize the law in fleeting moments where lives hang in the balance.[185] But difficult questions about the propriety of government investigatory techniques may be less amenable to settlement for settlement's sake.

Society gains relatively little by deciding permanently, but incorrectly, the limit of the government's warrantless data-collection techniques. If citizens never change their practice of driving on the right side of the road, they gain roadway safety at little cost to their freedom of choice. But if government investigators never change their practice of warrantlessly obtaining certain kinds of information about citizens, they gain only marginal ease in their investigations at huge costs to the privacy and tranquility of millions of citizens. Third-party doctrine cases are not about split-second officer choices in the line of fire; rather, they concern deliberative choices officers make when deciding to undertake long-term information gathering. That topic does not warrant the promotion of stability for stability's sake.

Stare decisis also acts as a ratcheting mechanism to protect hard-fought societal gains. Where past generations struggled to establish immutable principles of Justice, bulwarks against unwise reconsideration are appropriate. Some commentators, such as the late Antonin Scalia, have argued that preservation of ancient societal gains is the whole purpose of constitutional law and that constitutions exist "to prevent change—to embed certain rights in

---

in fact more important that things be settled than that they be settled right—the fact of settlement alone is enough to make the provision binding.").

[185] For example, consider exceptions to the warrant requirement based upon exigent circumstances or officer observation of criminal activity in public view, where there is a heightened possibility that evidence will be destroyed rapidly or other members of the public will be placed in harm's way if officers fail to respond immediately.

such a manner that future generations cannot readily take them away."[186]

But the Court does not protect hard-fought societal gains by granting government investigators permanent permission to warrantlessly access classes of information. Decisions on the reach of the third-party doctrine, if imbued with the full force of stare decisis, may do the opposite. How citizens and service providers use, collect, and interpret information changes, often in dramatic ways, over decades and centuries, making rulings in the area necessarily contingent. Supreme Court Justices are as unlikely to predict accurately how the government should access and collect information in the future as they are to predict accurately how tomorrow's citizens and service providers may create new solutions to emerging problems of daily life. No Justice should fancy herself a prognosticator of the next great technological advance or consumer need.[187] Instead, the Justices ought to humbly acknowledge that their rulings on the doctrine will almost certainly require adjustment in the future and hence openly admit that the decisions they make are provisional.[188]

When properly cast as provisional, rulings on the limits of new government data-collection capacities would work much like judicially enforced constitutional sunsets, a concept others and I have argued for in the past. In those scenarios, the Court might write an opinion expressly limiting that opinion's stare decisis effect to a set period or until a designated event, after which neither lower courts nor the Supreme Court would be bound by it.[189] "Sunsets thereby invite relitigation" as the sunset approaches and the

---

[186] Antonin Scalia, *Common Law Courts in a Civil Law System: The Role of United States Federal Court in Interpreting the Constitution and Laws*, *in* A MATTER OF INTERPRETATION, *supra* note 180, at 40.

[187] *See* FRIEDMAN, *supra* note 85, at 258 ("Rapidly advancing technology has gotten us into this pickle. Hard-to-change rules adopted by judges lacking in expertise is not the way to get us out.").

[188] *See id*. at 232–33 ("In the face of rapidly changing technology, what is required of judges is caution, some humility about their ability to understand what expectations of privacy society deems reasonable, and deference to democratic processes."); Gentithes, *Precedent*, *supra* note 186, at 853 (discussing the importance of judicial humility).

[189] Michael Gentithes, *Sunsets on Constitutionality & Supreme Court Efficiency*, 21 VA. J. SOC. POL'Y & L. 373, 380–81 (2014) (quoting Neal Katyal, *Sunsetting Judicial Opinions*, 79 NOTRE DAME L. REV. 1237, 1244–45 (2004)) ("[T]he Court can hand down an opinion and announce that its holding is entitled to the full effect of stare decisis for a set number of years. . . or that it will be binding law until a designated event. . . .").

principles guiding the decision are re-opened for debate.[190] The same could be true of rulings on the limits of the third-party doctrine. When the Court rules that some current privacy protections are important enough to maintain for at least the foreseeable future, it should leave open the possibility of revisiting its holding as changes in social mores and society-wide behavior dictate.

Though the Court has not consistently adopted this approach when considering new extensions of the third-party doctrine, it seemed to do so when it considered technological advances that allow investigators to obtain new information directly, rather than requesting it from a third party. For instance, the Court considered "what limits there are upon the power of technology to shrink the realm of guaranteed privacy" in *Kyllo v. United States*, where investigators used heat sensors to detect an indoor marijuana farm.[191] There, the Court focused upon the likely advance of surveillance technology: while the heat-sensors were "relatively crude," the Court noted that "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[192] If the government's technological advance

---

[190] *Id.* at 381. I have defended such judicially enforced constitutional sunsets on several normative grounds, each of which broadly fall under the rubric of efficiency:

> First, I argue that constitutional sunsets will allow the Court to more readily reach constitutionally accurate decisions in close and controversial cases by reducing the information deficit facing the Justices in those matters. Second, I describe the externalities created by repetitive constitutional litigation that fails to produce meaningfully new and useful constitutional rules and argue that they can be reduced through the use of constitutional sunsets, which if wielded properly, will reduce that type of low-value repetitive litigation in the first place. The reduction in these external costs will benefit the Court itself, the litigants before it, and the political branches. Third, constitutional sunsets will allow the Court to more efficiently reach larger majorities and thereby issue more stable and lasting opinions. Finally, constitutional sunsets will allow the Court to reach decisions not just more acceptable to those within the judiciary but to society in general because those decisions will mark a significant advance in terms of the Rule of Law values of clarity, publicity, and stability.

Id. at 394.

[191] 533 U.S. 27, 34 (2001).

[192] *Id*. at 36; *see also* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

intruded upon historical expectations of privacy in the home, the Court needed to limit the government's new capabilities to prevent "police technology [from] erod[ing] the privacy guaranteed by the Fourth Amendment."[193] The Court thus fashioned a rule prohibiting warrantless collection of information about the interior of a home obtained by sense-enhancing technology, "at least where . . . the technology in question is not in general public use."[194]

The *Kyllo* test is candidly provisional. A constitutional rule that looks to broad public use of a technological advance is one that everyone, including the Justices who formulated it, knows will change over time. *Kyllo* is designed to respond to evolving social realities in the same way the Court's jurisprudence ought to respond when confronting new government information-gathering techniques.

Similarly, *Miller* should be viewed as a provisional ruling, especially given the modern changes in how financial transactions are conducted and recorded discussed above.[195] Recognizing *Miller* as a provisional decision would also render any new third-party-doctrine rulings under the two-step test I recommend subject to change. But that is an acceptable, even desirable, outcome. Those decisions determine whether information is sensitive enough to deserve at least some protection, a necessarily provisional holding. When the Court decides whether information is more like sensitive medical data or unprotected phone numbers, it is not prescient enough to know with certainty how collection of that information will affect citizens' daily affairs, especially as new technology emerges. Citizens may adapt new practices that render that information and its analogues more or less sensitive, requiring the Court to revisit its provisional holdings.[196]

---

193 *Kyllo*, 533 U.S. at 34; *see also id.* ("[I]n the case of the search of the interior of homes . . . there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." (emphasis in original)).

194 *Id.*

195 *See supra* Part II.D; *see also supra* note 158 and accompanying text.

196 *See* United States v. Miller, 425 U.S. 435, 452 (1976) (Brennan, J., dissenting) ("[J]udicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices." (quotation omitted)).

IV. RESOLVING THIRD-PARTY CONTROVERSIES WITHOUT *MILLER*

By excising *Miller* using my two-step sensitivity test, the Court can generate the flexibility it needs to address government acquisition of third-party records created by new technologies. It will allow the Court to comfortably explain the result in *Carpenter*, which addressed the collection of CSLI data generated by cell phone companies that show roughly where the customer was based on which cell tower a customer's phone accessed at a particular time.[197] The *Carpenter* majority excepted a week's worth of CSLI from warrantless collection under the third-party doctrine, opening the door for varying applications of the doctrine to "distinct categor[ies] of information."[198] However, the majority failed to clearly delineate the difference "between cell-site records on the one hand and financial and telephonic records on the other."[199]

Miller hinders the Court's resolution of *Carpenter*. *Miller* created a false dichotomy that did not depend on the underlying data's sensitivity, classifying information as either wholly protected, undisclosed data, or wholly unprotected data disclosed to a third party.[200] And *Miller* made clear that even moderately sensitive data, like financial information or one's locations in public, can be wholly unprotected.[201] Maintaining *Miller*'s holding on financial information forces a choice between unattractive options: either require a warrant each time the government collects any data about a citizen's locations from a third party or never require such a warrant, no matter how much locational data the government collects.[202]

---

197 Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

198 *Id*. at 2219.

199 *Id*. at 2221 (Kennedy, J., dissenting).

200 *See supra* Part I.A and II.B.

201 *See Miller*, 425 U.S. at 442–43 (discussing how there is no expectation of privacy in contents of original checks and deposit slips based on the Fourth Amendment interest in bank records).

202 *See* Levinson-Waldman, *supra* note 44, at 570

> [A]nyone who steps outside takes the risk that they may be seen, whether by a police officer or civilian, whether to the grocery store, the abortion clinic, or the NRA meeting. What they do not expect is that each of those moments will be recorded and kept in perpetuity for later discovery and analysis by a probing law enforcement officer, either wholesale or piecemeal.

But the Court did not make a choice between those unattractive options. Instead, it took a middle path, preserving the core of the third-party doctrine, including *Miller*, but excepting at least one, and potentially more, categories of information from straightforward alignment with *Miller*'s dichotomy between disclosed and undisclosed information.[203] That decision is a vital step towards a nuanced categorical approach, but is too tentative in dealing with *Miller*'s holding itself.

Instead, the Court should overturn *Miller*'s holding that sensitive information like financial data is not entitled to any Fourth Amendment protection when collected by third parties. This would leave in place the third-party doctrine that investigators have relied upon for over forty years, but adjust it by accounting for the sensitivity of some data types. The Court could hold that data like financial transaction records, much like CSLI, is sensitive enough to warrant some protection, placing each of those data categories closer to the center of a continuum between wholly protected and wholly unprotected information.

Excising *Miller* is necessary for the Court to adopt the informational sensitivity rationale that would have justified the *Carpenter* majority's analysis. It would allow the Court to adopt a clear framework to categorizing information for third-party doctrine purposes, giving a workable model for future analyses in the area.

If the Court applied this two-step test , the outcome in *Carpenter* would be the same, but the analysis would be far clearer. First, the Court could determine the sensitivity of long-term location information like CSLI by looking to its own jurisprudence as well as the substantive meaning that the information conveys on its face.[204] In the case of long-term location information, the Court's jurisprudence has suggested that it might be particularly sensitive. In *Jones*, Justice Alito noted that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[205] Two years later, Chief Justice Roberts

---

[203] *See Carpenter*, 138 S. Ct. at 2217 ("We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

[204] For other illustrations of sensitivity determinations, see *supra* Part II.C and II.D.

[205] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

similarly intimated the unique sensitivity of location information. When discussing whether police officers could warrantlessly search the contents of a cell phone seized incident to an arrest in *Riley*, Roberts noted that "[d]ata on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[206] These nuggets of related jurisprudence suggest the sensitivity of location information.

Likewise, long-term location information conveys significant meaning on its face. Knowledge of a citizen's locations reveals a great deal about her life. It might show how she worships, whether she suffers from physical or mental ailments, and which political party she supports.[207] It can reveal patterns inimical to sensitive personal relationships she privately maintains with others—the unique "intimate window into a person's life" that the *Carpenter* majority emphasized.[208] Furthermore, a citizen's mere knowledge that she may be under constant surveillance necessarily curbs her expressive behavior, even if the government has not actually been watching.[209] Long-term location information conveys significant, sensitive information on its face. That inherent meaning, along with the Court's prior treatment of location information, suggests that CSLI ought to be placed towards the more sensitive side of the continuum I propose, and receive some Fourth Amendment protection.[210]

CSLI is also sensitive because of the ubiquity of cell phones in modern life. Though perhaps not required, devices that rely upon

---

[206] 134 S. Ct. 2473, 2490 (2014) (citation omitted).

[207] *See supra* note 202 and accompanying text. Though it may be unknowable to the government investigator ex ante, some particular location data points are especially sensitive, such as the trip to the abortion clinic or the by-the-hour motel. The mosaic theory's concern, in part, is the likelihood that long-term surveillance will inevitably capture a few of those especially sensitive data points. *See* Smith, *supra* note 93, at 580–81.

[208] *Carpenter*, 138 S. Ct. at 2217.

[209] Gray & Citron, *supra* note 18, at 76–77 (arguing that individuals "internalize the notion of being watched, even if it is not actually happening").

[210] *Cf.* SCHULHOFER, *supra* note 11, at 141 ("The major aim of the Fourth Amendment—unquestionably—is not to bolster majority rule but to afford shelter to political, religious, and ideological minorities. It would surely astonish the Framers—not to mention those who feel targeted for surveillance today (observant Muslims, for example)—to discover that the Fourth Amendment affords no protection against spying tactics . . . .").

signals relayed through cell site towers are so commonplace that their use is only marginally voluntary. Cell phone use is "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society."[211] Though this does not defeat the application of the third-party doctrine to such information, it does inform the sensitivity judgment that will help define that doctrine's limits regarding CSLI.

Second, the Court could consider the amount of CSLI data that the police sought. Because CSLI is sensitive, government collection of significant amounts paints an informational mosaic of the defendant and constitutes a search. The CSLI in *Carpenter* gave the government a crystallized image of the defendant's daily life. And given the high sensitivity of CSLI, that was plainly more invasive to his privacy than the Fourth Amendment permits. As Justice Alito noted in *Jones*, "society'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."[212] In *Carpenter*, the government obtained just such a catalogue using signals emitted from a device ubiquitous in most of our lives today. Such warrantless activity violated the Fourth Amendment under my two-step test. While the collection of one or even several CSLI data points may not constitute a Fourth Amendment search, the amalgamation of unlimited amounts of CSLI creates such a detailed mosaic of a citizen's life that it invades her reasonable expectations of privacy and triggers the Fourth Amendment's warrant requirement.

By affording some protection to CSLI but retaining the third-party doctrine using the informational sensitivity rationale, the Court can ensure that the Fourth Amendment serves not just law enforcement interests, but also the privacy concerns of the common man. This refocuses professor Orin Kerr's influential view that the Justices seek equilibrium between police officers and criminals in the Fourth Amendment. As Kerr argues, the Court uses a "correction mechanism" when either "changing technology or social practice makes evidence substantially harder" or "substantially

---

[211] *Carpenter*, 138 S. Ct. at 2217 (quotation omitted).

[212] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

easier for the government to obtain."[213] In the latter scenario, "the Supreme Court often embraces higher protections to help restore the prior level of privacy protection."[214]

Kerr's theory overemphasizes a game played only by the police and criminals. According to Kerr, new technologies "threaten the privacy/security balance because they enable both cops and robbers to accomplish tasks they couldn't before, or else to do old tasks more easily or cheaply than before."[215] This view wrongly suggests that investigators must face a particular degree of difficulty when uncovering crime. The Fourth Amendment concerns more than just the guilty and those who prosecute them. If a normatively desirable "equilibrium" between those parties was the Amendment's aim, it would never limit the capabilities of investigators trying to catch bad guys. Supreme Court cases "have historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[216]

The Fourth Amendment protects the broader public against invasions upon their privacy and tranquility.[217] The Court's rulings protect hundreds of millions of innocent people in society, not just criminals. That society-wide concern should lead the Court to adjust the third-party doctrine for the rest of us. It should classify some information, such as the CSLI data in *Carpenter* or the financial data in *Miller*, as neither wholly protected nor wholly unprotected when collected by third parties. All citizens—not just criminals—use third party services that generate sensitive data every day, never imagining that the government might collect all that information on a whim.[218] In some amounts, the government may

---

[213] Kerr, *supra* note 11, at 480.

[214] *Id.*

[215] *Id.* at 486. "The police continuously devise new ways to catch criminals. Criminals continuously devise new ways to avoid being caught. This state of flux poses an underappreciated difficulty for judges interpreting the Fourth Amendment." *Id.* at 481.

[216] Riley v. California, 134 S. Ct. 2473, 2493 (2014) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

[217] *See* Gentithes, *supra* note 11, at 939.

[218] It is worth noting that the majority of citizens may not understand how CSLI is generated. Recent surveys indicate

> that the majority of cell phone users do not know that their cell phone provider collects their location data, and roughly 15% of users affirmatively

collect that data warrantlessly; in others, such as where the government amalgamates troves of highly sensitive data, it should first obtain a warrant based upon probable cause.

CONCLUSION

Though the third-party doctrine may not be doomed, it desperately needs adjustment in a modern, networked world. Neither instinctively touting it as an absolute rule nor bashing it as a misunderstanding of the way modern citizens disclose information to service providers will provide the needed adjustment. Instead, the Supreme Court should end *Miller*'s time at the forefront of the doctrine, allowing the doctrine to account for the sensitivity of disclosed information. Sensitive information, like financial data or CSLI, should receive some protection even after it is conveyed to third parties. Warrantless collection of individual points of such sensitive information may be permissible, but the Court should require a warrant before government investigators can amalgamate enough such data to paint a detailed mosaic of a citizen's life.

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

Tokson, *supra* note 47, at 177. However, what citizens actually know about how data is gathered by third parties might not actually drive the Court's reasoning in these cases. "The rhetoric of knowledge may . . . mask the normative judgment that actually drives the decision." *Id.* at 151.