PRIVILEGING PRIVACY: CONFIDENTIALITY AS A SOURCE OF FOURTH AMENDMENT PROTECTION

*Mihailis E. Diamantis**

ABSTRACT

Police generally do not need a warrant to search information that we reveal to third parties. This so-called "third-party doctrine" is supposed to tell courts when our personal information is no longer private, and therefore not protected by the Fourth Amendment. In the modern world, the doctrine goes too far, leaving much of our most intimate information exposed. We have little choice but to trust third-parties like cell companies, internet service providers, email providers, and the like with most of the data we generate.

The root of the problem is the Supreme Court's restrictive conception of privacy. As the third-party doctrine shows, the Court inherently understands privacy to be a type of secrecy. Just as information is no longer secret when told, the Court thinks that information is no longer private after it is shared. The narrow exception recently recognized in Carpenter v. United States does little to change this. In response, scholars have tried to invent entirely new conceptions of privacy or have proposed overruling the third-party doctrine altogether.

There is no need for such drastic and unlikely measures. Anglo-American law already has a suitable alternate understanding of privacy, refined over a four-hundred-year tradition, that is up to the task. Long before privacy was important to constitutional law, it was one of the central concepts for the common law of attorney-client privilege. Importantly, the privilege takes privacy to be a kind of confidentiality, rather than secrecy. Confidences, unlike secrets, can be shared. As a result, attorney-client communications can remain privileged even after voluntary disclosure to third parties if appropriate steps were taken to preserve their confidentiality. Conceiving of privacy as a kind of confidentiality could help soften the bright-line of the third-party doctrine by recognizing when the presence of third parties like cell companies or email providers truly removes privacy interests, and, as importantly, when it does not. Without such a development, the third-party doctrine will not survive the Information Age—or our Fourth Amendment protections will not survive it.

TABLE OF CONTENTS

INTRODUCTION 486

I. FOURTH AMENDMENT SECRETS 492
  A. The Third-Party Doctrine 492
  B. Scholarly Criticism 501

II. ATTORNEY-CLIENT CONFIDENCES 507
  A. Background to the Attorney-Client Privilege 508

* Associate Professor, University of Iowa, College of Law. I owe thanks to Todd Pettys for invaluable comments, to participants at Constitutional Law Colloquium at Loyola University Chicago for early encouragement and advice, and to my research assistant Derek Huish for many hours of excellent work.

B. Confidentiality and Third Parties 512

III. REASONABLE EXPECTATIONS OF CONFIDENTIALITY 521
A. An Open-Textured Inquiry 523
1. Subjective Expectation 524
2. Objective Reasonableness 528
B. Test Case: Carpenter v. United States 533

CONCLUSION 541

INTRODUCTION

> If you have me, you want to share me. If you share me, you haven't got me. What am I?
>
> —Old Riddle[1]

We generate at least two-and-a-half quintillion bytes of data every day.[2] Common sense dictates that much of this information—private photos, personal documents, geolocation records, communications with friends and family, etc.—is just the sort of thing that the Fourth Amendment should presumptively protect.[3] It does not. Because most of this information passes through wires, servers, and satellites that others own, it is beyond the reach of the Fourth Amendment.[4] The need to protect this information from those with the power to punish was one of the crucial insights of the warrant requirement.[5] When authorities have ready access to our private information, we lose the open-ended freedom to develop and explore the diverse personal identities that are the cornerstone of American individualism and progress.[6]

---

1 *See, e.g.*, Ivan Dimitrijevic, *Answer These Riddles and You Will Find the Answers to Life*, LIFEHACK, https://www.lifehack.org/articles/communication/answer-these-riddles-and-you-will-find-the-answers-life.html.

2 Matthew Wall, *Big Data: Are You Ready for Blast-Off?*, BBC NEWS (Mar. 4, 2014), http://www.bbc.com/news/business-26383058. This number is almost three years old now; it is surely much higher today.

3 U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

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

5 *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("[T]he [Fourth] Amendment seeks to secure the 'privacies of life' against 'arbitrary power.'" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)); Johnson v. United States, 333 U.S. 10, 13–14 (1948) (explaining that the purpose of the warrant requirement is to limit invasions of privacy by law enforcement).

6 ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION 28 (2013) ("[P]rivacy being the realm that is meant to be one's own domain, the territory of one's undivided

Not for the first time, Supreme Court doctrine developed at an earlier stage of human technology is bungling things today. In the nineteenth century, Fourth Amendment doctrine centered on preventing unwarranted physical intrusions by the government.[7] With the advent of wired telecommunications in the twentieth century, the physical intrusion test regretfully led the Court to bless forty years of unwarranted police wiretaps[8] before changing its approach.[9]

In the present day, the doctrinal holdover is the third-party doctrine. The current touchstone of Fourth Amendment protection is sensible enough; it safeguards citizens' "reasonable expectation[s] of privacy."[10] The qualification added by the third-party doctrine may itself have made sense when the Supreme Court announced it decades ago: "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[11] Today, in the connected world of cellphones, tablets, and laptops, that information is almost *all* of it. To make use of these devices, we have to trust everything passing to or from them to the third parties who transmit and store our data.[12] Under the third-party doctrine, this means

---

sovereignty, inside which one has the comprehensive and indivisible power to decide 'what and who I am' . . . . ").

7 *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356 (1974) (discussing that, traditionally, "searches" included physical entries and intrusions, but did not include observations without physical intrusion).

8 *See* Olmstead v. United States, 277 U.S. 438, 464 (1928). Justices in the dissent saw the danger of the approach. *Id.* at 474 (Brandeis, J., dissenting) ("The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?").

9 Katz v. United States, 389 U.S. 347, 359 (1967) (holding that governmental activities of wiretapping to listen to individual phone calls at a telephone booth violated the Fourth Amendment of the Constitution).

10 *Id.*; City of Ontario v. Quon, 560 U.S. 746, 765 (2010) (holding that a city police officer's employer did not violate the Fourth Amendment by reviewing the officer's cell phone text messages because the officer did not have a reasonable expectation of privacy in sending the text messages); New York v. Class, 475 U.S. 106, 117 (1986) (holding that police officers did not violate the Fourth Amendment by reaching into the defendant's car to find a VIN number of his automobile because the defendant did not have a reasonable expectation of privacy in locating the VIN number).

11 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

12 *See* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 24–25 (2017) (discussing different ways that information is taken from unwitting technology users during the course of modern life); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 211–12 (2006) (discussing "pervasive, ubiquitous data collection" and storage in modern society).

that information has no Fourth Amendment protection.[13]

The Supreme Court's recent decision in *Carpenter v. United States* does little to change this.[14] In *Carpenter*, the Court was asked whether police need a search warrant to access hundreds of days of "historical cell phone records that provide a comprehensive chronicle of the user's past movements."[15] The Court left the third-party doctrine intact,[16] but created a "narrow" exception for seven-day blocks of cell-site-derived geolocation data.[17] All other sorts of data, even the same geolocation data in six-day blocks, are unaffected by the opinion.[18]

What is needed is a principled way of distinguishing between those cases where the third-party doctrine makes sense, and those where it does not. Sometimes it *does* make sense. It is hard to maintain that the things someone says loudly to the person seated beside her on a crowded subway are still truly private.[19] But there is an obvious difference when that someone is speaking in her own home, and the "third party" is a cell company's algorithm logging the call.

Others have criticized the privacy gap in Fourth Amendment jurisprudence[20] and proposed remedies. Some have called for abandoning the third-party doctrine as anachronistic.[21] That extreme solution risks abandoning the sensible results of the doctrine and unnecessarily hampering police investigations where no real privacy interests are at stake.[22]

---

13 *See, e.g.*, *Smith*, 442 U.S. at 745–46 (holding that phone records may not protected); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that bank records may not be protected); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 93 (2011) ("So does the Fourth Amendment protect you when the Government seeks your Google search records? Not at all."). *But see* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (holding that compelling internet records that an internet provider produced without obtaining a warrant is a violation of the Fourth Amendment).

14 138 S. Ct. 2206 (2018).

15 *Id.* at 2211–12.

16 *Id.* at 2220 ("We do not disturb the application of *Smith* and *Miller* . . . .").

17 *Id.*

18 *Id.* at 2220–21 ("We do not express a view on matters not before us . . . . Nor do we address other business records that might incidentally reveal location information.").

19 Lee Humphreys, *Social Topography in a Wireless Era: The Negotiation of Public and Private Space*, 35 J. TECHNICAL WRITING & COMM. 367, 367 (2005) ("Talking on the phone is usually a private activity, but it becomes a public activity when using a cellphone in certain spaces.").

20 Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 532 (2013) (discussing the "gaps" in the constitutional protection provided by the Fourth Amendment).

21 Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 142 (2014) (discussing that the third-party doctrine's role in the Fourth Amendment is "anachronistic to serve their purpose of distinguishing the borders of privacy protection.").

22 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600–01 (2009)

A different sort of solution would call for reforming the doctrine from the inside out. Perhaps a new theory of privacy could get judicial buy-in, and lead to a more sensible third-party doctrine based off it.[23] As argued below, the Supreme Court's hair-trigger conception of privacy as a kind of secrecy—lost when shared with someone else—is problematic. A different understanding of privacy could generate a third-party doctrine with a more discriminating touch. But before going to the lengths of inventing a new approach to privacy, we should consider whether there is not another solution, ready-made, and already a familiar fixture of Anglo-American legal traditions. Not only would such a solution save a lot of effort, but the creatures of habit who run our courtrooms would likely be more receptive to it.

This Article approaches the problem by drawing on an area of law that privacy scholars have too long overlooked—attorney-client privilege. Embedded in attorney-client privilege jurisprudence is our longest-standing and richest privacy law tradition. The attorney-client privilege is a common-law protection for private communications between an attorney and her client.[24] If protected by the privilege, courts cannot force the attorney or the client to turn over information, whether to other private parties or to the government. The crucial element of the privilege is that the communications must be confidential.[25]

There is a version of the third-party doctrine at play in attorney-client privilege too—communications may lose their confidential nature if they are made in the presence of, or are subsequently disclosed to, third parties. The important difference is that, depending on the context, there are steps attorneys and clients can take that will preserve the confidentiality of their communications. As a general rule, with basic appropriate precautions, the attorney-client privilege protects information even after disclosure to third parties like email providers, cell companies, and internet service providers.

Courts applying privilege figured out decades ago what the Supreme Court still has not—how to treat information as private after it is shared with third-party service providers. In the early rules and doctrines governing attorney-client confidences are the tools we need to adapt the Fourth

---

(advancing that the third-party doctrine is important to maintain balance between police investigatory efforts and the privacy rights of citizens).

23 *See, e.g.*, STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 8–9 (2012) (proposing one such theory).

24 FED. R. EVID. 501.

25 *See* 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2292, at 554 (John T. McNaughton rev., 1961) (noting requirement that attorney-client communications be "made in confidence" in order to be privileged).

Amendment and the third-party doctrine to the modern day. The solution is practical and readily implemented, without grand shifts in fundamental Fourth Amendment jurisprudence or revisionary theories of privacy.

In the lead-up to *Carpenter*, the Supreme Court seemed poised to recognize something like the secrecy/confidentiality distinction. Individual members of the Court had signaled their discomfort with the third-party doctrine in separate opinions.[26] Judge Stranch, who sat on the Sixth Circuit panel below, wrote a begrudging concurrence that asked the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[27]

The *Carpenter* Court nearly hit on a re-conception of the third-party doctrine. It struggled for a vocabulary to describe situations in which "third parties [hold] records in which the suspect has a reasonable expectation of privacy."[28] Failing to find it, the Court tried a different tactic—an artificial carve-out for the "rare case[ ]" of seven-day blocks of cell-site location information—"an entirely different species of business record."[29] As Justice Kennedy argued in dissent, this distinction has the ad hoc feel of "an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other."[30]

The language the Court needed was the language of confidentiality. With that in hand, a solution to the third-party problem that does not rely on unsupportable distinctions between types of business records would have come into view.[31] The Fourth Amendment does not protect some fore-ordained categories of "persons, houses, papers, and effects" over others.[32] Rather, as the Supreme Court has recognized for the last half century, the Fourth Amendment protects information in which people have privacy interests.[33] As argued below, modern technology is forcing us to distinguish between types of

---

26 *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." (internal citations omitted) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976))).

27 United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016) (quoting *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring)), *rev'd*, 138 S. Ct. 2206 (2018).

28 Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

29 *Id*. at 2222.

30 *Id.* at 2224 (Kennedy, J., dissenting).

31 *Id.* at 2220 (majority opinion) ("We do not express a view on matters not before us . . . . Nor do we address other business records that might incidentally reveal location information.").

32 U.S. CONST. amend. IV.

33 *See generally* Katz v. United States, 389 U.S. 347 (1967) (introducing the reasonable expectations of privacy test).

privacy interests that were too easy to conflate not long ago. The interests the Fourth Amendment should protect are confidentiality, not secrecy.

This Article explores what lessons the law of privilege, and in particular its understanding of privacy as a type of confidentiality, holds for Fourth Amendment jurisprudence. There are notions of voluntariness, disclosure, precaution, and fairness at play in the privilege context that have yet to find their way into the constitutional privacy literature. What is more, these notions are backed by centuries of jurisprudence and doctrine that could be imported with little modification into the Fourth Amendment inquiry. This Article begins (Part I) by laying out the law behind the third-party doctrine and its problematic conception of privacy as a kind of secrecy. That Part also discusses *Carpenter* and some other representative solutions others have proposed, along with their significant shortcomings. The Article then detours through an examination of privacy-as-confidentiality in the law of attorney-client privilege, emphasizing how it relates to third-party disclosures (Part II). In its main substantive contribution, the Article weaves these two doctrinal threads together to show how Fourth Amendment jurisprudence would benefit from viewing privacy as a kind of confidentiality (Part III). This development would allow the third-party doctrine to distinguish more meaningfully between cases when sharing information with a third party relinquishes one's privacy interests, and, as importantly, when it does not. In the course of discussing the detailed mechanics of a Fourth-Amendment confidentiality inquiry, the Article considers how it could have played out in *Carpenter v. United States*; the Court could have reached the same ruling, but with firmer theoretical foundation and more helpful guidance to lower courts who will, after *Carpenter*, be "kep[t] . . . guessing for years to come."[34]

The argument below proceeds in the terms set by the Supreme Court and most Fourth Amendment scholars. That discussion has been largely policy- and political-philosophy-oriented, and ahistorical.[35] The central interpretive concept—privacy—is not directly mentioned in the Constitution. While there is certainly interpretive value that rigorous originalist or textualist methods could bring to the questions addressed here, the Article does not consider them. Rather, it seeks to validate the values recognized by the Supreme Court's Fourth Amendment jurisprudence. It does this by working within (to the extent possible) the Supreme Court's

---

34 *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting).

35 *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 552 (1999) ("The modern interpretation of 'unreasonable searches and seizures' is the product of post-framing developments that the Framers did not anticipate.").

present Fourth Amendment conceptual and doctrinal framework.

I. FOURTH AMENDMENT SECRETS

The Fourth Amendment shields our personal information from scrutiny by authorities.[36] It guarantees our right to be secure in our "persons, houses, papers, and effects, against unreasonable searches and seizures."[37] Its protection is not absolute, however. Authorities can still access that information if they have a warrant supported by "probable cause."[38] Furthermore, there is some personal information that the Fourth Amendment does not protect.[39] This division—between unprotected personal information, personal information subject to a warrant, and personal information authorities cannot access—is the Constitution's way of balancing individual privacy interests and the public interest in investigating misconduct.[40] This Part discusses the concept underlying the line the Supreme Court has drawn between unprotected and protected information: secrecy.

A. The Third-Party Doctrine

The foundation of Fourth Amendment protection is the people's "reasonable expectation of privacy" in their bodies, spaces, and information.[41] Where a search would violate those expectations, the government must first obtain a warrant, backed by "reasonably trustworthy information" that the search will turn up evidence of crime.[42] There is no certain means of predicting when and over what someone has a reasonable expectation of privacy.[43] As the phrase suggests, inquiry into reasonable expectations of

---

36 U.S. CONST. amend. IV.

37 *Id.*

38 *Id.*

39 *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 121–22 (1984) (holding that, with regard to a police search and seizure of a package containing contraband, "it is well settled that it is constitutionally reasonable for law enforcement officials to seize 'effects' that cannot support a justifiable expectation of privacy").

40 *See* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (holding that the Fourth Amendment must balance an "individual's legitimate expectations of privacy and personal security" with the government's "need for effective methods to deal with breaches of public order").

41 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *see* Rakas v. Illinois, 439 U.S. 128, 143 (1978); United States v. Chadwick, 433 U.S. 1, 7 (1977); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. Dionisio, 410 U.S. 1, 14 (1973); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968).

42 Brinegar v. United States, 338 U.S. 160, 175–76 (1949).

43 *See* Samson v. California, 547 U.S. 843, 848 (2006) (holding that the Court will evaluate the "totality

privacy has both subjective and objective dimensions. To begin, a person claiming Fourth Amendment protections must have had an actual, subjective expectation of privacy in the information.[44] This requires that she believe the information is and should be private and that she seek to preserve its privacy.[45] The second, objective dimension asks whether her subjective expectation is "one that society is prepared to recognize as 'reasonable.'"[46] Neither dimension seems to be particularly principled in its application. There are few bright-line tests outside of some core cases, like the presumed privacy of things within the home.[47] In cases beyond the core, the Court usually channels its often-outdated intuitions about what "people in general" think about privacy.[48] One might expect that sociological data about evolving notions of privacy would assist the Court's analysis, especially with respect to the objective prong of the inquiry. Some Fourth Amendment scholars are starting to collect such evidence (especially as it pertains to electronic communications),[49] but it has yet to find its way into Court opinions.[50]

Though the Court's positive notion of privacy is frustratingly hard to pin down, the negative limits on what counts as private speak volumes. The Court has recognized various circumstances in which a person has no reasonable expectation of privacy. The "plain view" doctrine, for example, states that a person has no reasonable expectation of privacy in items or information that are plainly visible to police conducting an otherwise legitimate search.[51] Similarly, the Court has held that people have no

---

of the circumstances" when determining whether conduct breaches a person's reasonable expectation of privacy (quoting United States v. Knights, 534 U.S. 112, 118 (2001)).

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

45 *Id.* at 351 (majority opinion).

46 *Id.* at 361 (Harlan, J., concurring).

47 Payton v. New York, 445 U.S. 573, 586 (1980) ("[S]earches and seizures inside a home without a warrant are presumptively unreasonable."); *see also* Florida v. Jardines, 569 U.S. 1, 14–15 (2013) (holding that, as a bright-line rule, the use of a device not in public use to search details of a home that are not otherwise exposed to the public violates the Fourth Amendment).

48 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979) ("First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial."). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting) ("Politically insulated judges come armed with only the attorneys' briefs, a few law clerks, and their own idiosyncratic experiences. They are hardly the representative group you'd expect (or want) to be making empirical judgments for hundreds of millions of people. Unsurprisingly, too, judicial judgments often fail to reflect public views.").

49 Milton Heumann et al., *Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace*, 14 RUTGERS J.L. & PUB. POL'Y 37, 75 (2016) (discussing findings about the public perception of technological surveillance and privacy implications on the Fourth Amendment).

50 *See* L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2035–41 (2011) (arguing against judicial reliance on legal assumptions rather than empirical data in Fourth Amendment jurisprudence).

51 Arizona v. Hicks, 480 U.S. 321, 325–26 (1987); *see also* Horton v. California, 496 U.S. 128, 133

reasonable expectation of privacy in things held out to the public, like their street-side garbage.[52] These legal doctrines about what privacy is *not* begin to suggest an implicit conception of what the Court thinks privacy *is*. The key to privacy seems to be non-exposure, i.e., keeping items and information hidden from view.

The most constraining doctrinal limit on privacy is also the most illuminating. According to the third-party doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[53] The thought behind the third-party doctrine is that if a person is willing to share some information with other people, she cannot have really thought (and society is not prepared to recognize) that it was really all that private in the first place. In a lot of cases, based on circumstances and who the third parties are, the third-party doctrine makes a lot of intuitive sense. For example, the third-party doctrine applies to business and tax records that a defendant turns over to an accountant whom she knows has a mandatory duty to report.[54]

The Supreme Court has affirmed and extended what many had thought were the outer limits of the third-party doctrine's logic. These often are cases where people must rely on third-party service providers for basic aspects of their shared social and economic lives. There were signs that the third-party doctrine could undermine Fourth Amendment interests as early as 1976, when the Court held that a person's bank records are not subject to the warrant requirement.[55] The bank, after all, is a third party. This holding stands today, despite widespread recognition in the law that people have privacy interests in their financial information.[56]

Similar reasoning in the following century established that phone records are not protected.[57] Bank and phone records represent information in which it is at least debatable (Supreme Court rulings aside) whether people have a

---

(1990) ("If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy.").

52 California v. Greenwood, 486 U.S. 35, 40 (1988) ("Here, we conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection.").

53 *Smith*, 442 U.S. at 743–44.

54 Couch v. United States, 409 U.S. 322, 335 (1973) (holding that turning over business and tax records to an accountant who was known to be duty-bound to report information negates a defendant's reasonable expectation of privacy in the records).

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

56 *See* Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, 15 U.S.C. §§ 6801–09 (2012).

57 *Smith*, 442 U.S. at 743–44 (describing how the petitioner, by voluntarily conveying numerical information to the telephone company, "can claim no legitimate expectation of privacy").

reasonable expectation of privacy.[58] The third-party doctrine gave the Court an easy answer that allowed it to ignore difficult implications. Today, it would apply to email accounts run by Microsoft or Google and to DNA data from services like 23andMe.[59]

The Supreme Court does recognize that the third-party doctrine may not always make sense. In one important limitation, the Court held that privacy interests survive where, unknown to parties claiming the protections of the Fourth Amendment, the third party with access to their information was acting at the direction or encouragement of the government.[60] Such third parties are "instrument of state" who are basically operating like covert government agents.[61] Access by them does not compromise people's privacy interests vis-à-vis the government because there is effectively no real third party. Typical cases involve luggage handlers[62] or hotel employees[63] who, prompted by a federal investigator looking on, open customer bags or rooms to search for narcotics. In these cases, the third party would not have pried into private information but for the government's involvement. Allowing police to circumvent the warrant requirement by engaging their own third parties would undermine basic Fourth Amendment protections.

The most recent limit on the third-party doctrine came this year in *Carpenter*. The Court reaffirmed its commitment to the third-party doctrine,[64] but was asked how to extend it to cell-site data which "chronicle[s] a person's past movements through the record of his cell phone signals."[65] A

---

58 *See Miller*, 425 U.S. at 446–47, 455 (Brennan, J., dissenting) (discussing disagreement between majority and dissenting Justices on whether bank records are protected by the Fourth Amendment); *see also Smith*, 442 U.S. at 748, 752 (Marshall, J., dissenting) (discussing disagreement between majority and dissenting Justices on whether phone records are protected by the Fourth Amendment).

59 *See* Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) (discussing the troubling breadth of the third-party doctrine).

60 *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

61 *See id*. (referring to the wife of the defendant as potentially being "an 'instrument' or agent of the state" in a police investigation).

62 *See* United States v. Doe, 61 F.3d 107, 109 n.3 (1st Cir. 1995) (holding that airport security actions implicate the Fourth Amendment when security checkpoint personnel are acting pursuant to federally prescribed regulations and directives).

63 *See* United States v. Reed, 15 F.3d 928, 933 (9th Cir. 1994) (holding that a search of a hotel room performed by a hotel employee, while working with the police, amounted to state action implicating the Fourth Amendment).

64 *See Carpenter*, 138 S. Ct. at 2216 ("We have previously held that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.' That remains true 'even if the information is revealed on the assumption that it will be used only for a limited purpose.'" (internal citations omitted) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976))).

65 *Id.*

straightforward application of the third-party doctrine would have found no Fourth Amendment protection since cell-site data is necessarily shared with third-party cell service providers.[66] The Court decided that, "[g]iven 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."[67] It is unclear what, if any, other sort of data shares that nature—its "uniqueness" suggests the answer may be none.[68] Indeed, after *Carpenter*, even cell-site location records are excepted from Fourth Amendment protection by the third-party doctrine so long as they cover less than seven days of data.[69] Given the extreme narrowness of *Carpenter*'s exception to the third-party doctrine, it does not impact the analysis below.

The logic and scope of the third-party doctrine suggest something about the Court's understanding of privacy. The third-party doctrine says (with rare exception) that when person *A* shares something with person *B*, it is no longer private. This is the informational logic of secrets.[70] Once information is provided to another person, its secrecy is compromised. The law recognizes this logic outside of the Fourth Amendment context. State secrets and trade secrets represent information that must not be shared, on pains of compromising the protections the law gives them.[71] Secrets are fragile and must be jealously guarded.

The practical impact of the Court's conception of privacy-as-secrecy was limited in the nineteenth and twentieth centuries, when the third-party doctrine was taking off. Social and economic structures were such that, with some exceptions like phone and bank records, relatively few transactions were memorialized. People could go about ordinary life interacting with the third parties they depended on in relative confidence that it did not matter that their exchanges may not be secret.

---

66 *Id.* at 2272 (Gorsuch, J., dissenting) ("I cannot fault the Sixth Circuit for holding that *Smith* and *Miller* extinguish any *Katz*-based *Fourth Amendment* interest in third party cell-site data.").

67 *Id.* at 2217 (majority opinion) (emphasis altered).

68 *Id.* at 2234 (Kennedy, J., dissenting) ("[T]he Court does not explain what makes something a distinct category of information [like cell-site data].").

69 *Id.* at 2217 n.3 (majority opinion).

70 SCHULHOFER, *supra* note 23, at 8–9 (arguing that the Court understands privacy as a form of secrecy).

71 Smith v. Dravo Corp., 203 F.2d 369, 373 (7th Cir. 1953) ("Of course, as the term [trade secret] demands, the knowledge cannot be placed in the public domain and still be retained as a 'secret'."); *see also* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1252, 1293 (2007) (arguing that a survey of state secret cases suggests that disclosure of information to the public would defeat the privilege).

Investigation and surveillance were expensive in-person affairs.[72] Without the aid of the sort of totalitarian information networks present in East Germany and the Soviet Union,[73] relatively few people could actually be people of interest. In the United States, there was safety in numbers. Budgetary and structural limits left plenty of room for most people to transact with each other, free from any real fear of unreasonable government searches into their personal lives.

Today is different in several respects. One important development of the twenty-first century is that third-party service providers have their own third parties. This is the interconnected world of Facebook and Venmo, where third-party service providers facilitate most social and economic transactions. Facebook and Venmo then implicate yet further third parties, like the cell service providers or ISPs through which we access their services. Every email we send, every website we visit, every file we store on the cloud, every credit card we swipe, and every phone call we make utilize several third-party platforms. As a result, the vast majority of government information requests to companies like cell carriers are not subject to the warrant requirement. Just obtaining subpoenas will often suffice,[74] and the process for securing these give your data relatively little protection.[75]

A second major development is that people now transmit information about themselves to third-party service providers, even when there is no obvious human or commercial counterparty. Walking alone on the sidewalk

---

72 Andy Greenberg, *Cell Phones Let Cops Track People for a Thousandth of the Price, Study Finds*, FORBES (Jan. 9, 2014, 6:50 PM), https://www.forbes.com/sites/andygreenberg/2014/01/09/cell-phones-let-cops-track-people-for-a-thousandth-of-the-price-study-finds/#7dcd88bf5e2e.

73 One person out of every sixty-six were government informants in East Germany. JOHN O. KOEHLER, STASI: THE UNTOLD STORY OF THE EAST GERMAN POLICE 9 (1999) (noting that one-in-sixty-six East Germans were government informants). The number in the U.S.S.R. may have been as high as one-in-ten. *Compare* ROBERT W. STEPHAN, STALIN'S SECRET WAR: SOVIET COUNTER-INTELLIGENCE AGAINST THE NAZIS 61 (2003) (noting that the U.S.S.R. may have had as many as twenty million informants), *with* Victor P. Petrov, *Some Observations on the 1959 Soviet Census*, 18 RUSSIAN REV. 332, 332 (1959) (citing the 1959 Soviet Census which put the population of the U.S.S.R. at over two-hundred million from 1959 onwards). Other estimates go as low as one in one hundred. For further information on Soviet information networks, see generally Amir Weiner & Aigi Rahi-Tamm, *Getting to Know You: The Soviet Surveillance System, 1939–57*, 13 KRITIKA: EXPLORATIONS RUSSIAN & EURASIAN HIST. 5 (2012).

74 Stored Communications Act, 18 U.S.C. § 2703(d) (2012); Letter from John C. Gockley, Vice-President, Legal & Regulatory Affairs of U.S. Cellular to Edward J. Markey, U.S. Senator (Oct. 1, 2013), *available at* https://www.markey.senate.gov/documents/2013-12-09_USCellular_CarrierResponse.pdf.

75 SOLOVE, *supra* note 13, at 93. There are some weak statutory protections for email and phone records, but these are changeable and do not provide the level of security ensured by the Fourth Amendment. *See* SCHULHOFER, *supra* note 23, at 128.

or room to room in their houses, people unwittingly take several third parties along with them if their phone happens to be in their pocket. Cell service providers track user location in real time,[76] as do the developers of the phone's apps—anything from flashlight apps[77] to innocuous-seeming games like Angry Birds and Candy Crush.[78] Sitting still while watching cat videos, researching vinyl siding, or trying to diagnose a rash, there is no obvious sign of the dozens of third-party marketers and their cookies who could be watching.[79]

A third major development is that our social and economic transactions are meticulously recorded and digitally searchable.[80] This all but eliminates the transaction costs of surveillance that, for much of the history of the third-party doctrine, were a practical shield for most personal information. Advertisers will pay top dollar for insights into people's preferences, and third-party service providers have responded in kind. Analysts like Sense Networks crunch personal cell-location data to make valuable user profiles.[81] Companies like Facebook generate user profiles from their own data, which can include over one thousand pages of text for each active user.[82] Other companies compile data from several service providers to package and sell. One such company, Acxiom, claims to have 1,500 data points on over

---

76 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) ("Most modern devices, such as smartphones, tap into the wireless networks several times a minute whenever their signal is on . . . ."). They are required by law to do this, though, as discussed *infra* pp. 499–500, there is a profit motive too. *See Fact Sheet: FCC Wireless 911 Requirements*, FCC (Jan. 2001), https://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf.

77 Ashley Feinberg, *Popular Android Flashlight App Straight-Up Lied About Selling Data*, GIZMODO (Dec. 6, 2013, 10:41 AM), http://gizmodo.com/popular-android-flashlight-app-straight-up-lied-about-s-1477916270.

78 Jordan Robertson, *Leaked Docs: NSA Uses 'Candy Crush,' 'Angry Birds' to Spy*, SFGATE (Jan. 29, 2014), http://www.sfgate.com/technology/article/Leaked-docs-NSA-uses-Candy-Crush-Angry-5186801.php (last updated Jan. 29, 2014, 5:07 PM).

79 *Fresh Air: Tracking the Companies that Track You Online*, NPR (Aug. 19, 2010, 11:00 AM), http://www.npr.org/templates/story/story.php?storyId=129298003.

80 *See Carpenter*, 138 S. Ct. at 2218 ("[T]he retrospective quality of [cell-site location information] gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection.").

81 Hiawatha Bray, *Cellphone Data Mined to Create Personal Profiles*, BOS. GLOBE (July 8, 2013), https://www.bostonglobe.com/business/2013/07/07/your-cellphone-yourself/eSvTK1UCqNOE7D4qbAcWPL/story.html.

82 Olivia Solon, *How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories*, WIRED (Dec. 28, 2012), http://www.wired.co.uk/magazine/archive/2012/12/start/privacy-versus-facebook.

700,000,000 people.[83] It should be unsurprising, then, that former Google CEO Eric Schmidt could honestly say, "We know where you are. We know where you've been. We can more or less [k]now what you're thinking about."[84] Third-party service providers record and compile personal information on a scale that was not technologically feasible a short while ago.

Some of the customers for this data are state and federal authorities. The third-party doctrine washes away any scruples about warrants and allows the government to purchase personal information that would have been prohibitively expensive to gather just decades ago. Third-party service providers cultivate lucrative and long-lasting commercial relationships with government buyers.[85] AT&T, for example, charges the government twenty-five dollars per day to track a phone,[86] and Sprint charges thirty dollars for a full month.[87] This is a fraction of the cost of traditional surveillance,[88] so police can send cell companies millions of data requests each year.[89] Cell companies have even developed automated web interfaces to keep up with demand.[90] For the federal government alone, intelligence contracts amount to $56 billion each year.[91] As one leading commentator observed, "corporate and government surveillance interests have converged."[92] It is the third-party doctrine that allowed them to.

If third parties are not willing to share customer information with police, the government often has the option of taking it, again without the need for a warrant. One common route is the Stored Communications Act, which

---

83 Adi Kamdar, *Data Broker Acxiom Launches Transparency Tool, but Consumers Still Lack Control*, ELEC. FRONTIER FOUND. (Sept. 12, 2013), https://www.eff.org/deeplinks/2013/09/data-broker-acxiom-launches-transparency-tool-consumers-lack-control.

84 Derek Thompson, *Google's CEO: 'The Laws Are Written by Lobbyists'*, ATLANTIC (Oct. 1, 2010), http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908.

85 Farhad Manjoo, *Acxiom Is Watching You*, SALON (Feb. 10, 2004, 8:30 PM), https://www.salon.com/2004/02/10/acxiom/.

86 Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (Dec. 4, 2012), https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data (last updated June 27, 2014, 10:29 AM).

87 Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 349 (2014).

88 Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) ("[C]ell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools.").

89 Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1.

90 Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html.

91 Tim Shorrock, Opinion, *Put the Spies Back Under One Roof*, N.Y. TIMES (June 17, 2013), http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html.

92 BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 29 (2015).

was at issue in *Carpenter*.[93] Passed in 1986, the Act allows the government to subpoena telecommunications records upon showing a judge "reasonable grounds to believe" the records are "relevant and material" to a criminal investigation.[94] Shortly after 9/11, the government acquired further subpoena powers. Congress passed the USA PATRIOT Act,[95] which amended the Foreign Intelligence Surveillance Act ("FISA") by weakening restrictions on domestic surveillance by the government. Domestic surveillance is now permitted so long as foreign intelligence gathering is a "significant purpose;" previously, it had to be "*the* purpose."[96] The National Security Agency understands the Act to allow them to send "national security letters" to corporations demanding the records, files, emails, etc., of their customers.[97] These FISA "requests" generally do not require a warrant; when they do, the secretive Foreign Intelligence Surveillance Court seems to grant them as a matter of course.[98] Companies that do not comply with national security letters face stiff penalties. In one instance, the National Security Agency threatened Yahoo with a fine of $250,000 per day if it refused to turn over user data; that figure was set to double every week.[99] After just two months, the fine would have been $64 million per day.

As a result of these developments, the third-party doctrine poses a widespread threat to much of people's most private information. The next Section considers various proposals about how Fourth Amendment law

---

93 Stored Communications Act, 18 U.S.C. § 2703(d) (2012); *Carpenter*, 138 S. Ct. at 2212.

94 18 U.S.C. § 2703(d).

95 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

96 § 218, 115 Stat. at 291 (second emphasis added).

97 *See* Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 525 (2006) ("[T]he 2001 USA PATRIOT Act . . . authorized a system of National Security Letters that the FBI has employed with increasing frequency in a wide variety of situations with only remote connections to the goal of preventing terrorism."); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1332 (2004) ("The Patriot Act significantly expanded the scope of the little-known tool of 'National Security Letters.'"); *see also* Russell L. Weaver, *Cybersurveillance in a Free Society*, 72 WASH. & LEE L. REV. 1207, 1237 (2015) ("[W]hen the NSA sends a National Security Letter to a telecommunications company, it usually includes an order precluding the company from publicly acknowledging the letters or the disclosures or even from alerting their customers.").

98 SOLOVE, *supra* note 13, at 130; Erika Eichelberger, *FISA Court Has Rejected .03 Percent of All Government Surveillance Requests*, MOTHER JONES (June 10, 2013, 5:30 PM), http://www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request; Colin Schultz, *The FISA Court Has Only Denied an NSA Request Once in the Past 5 Years*, SMITHSONIAN (May 1, 2014), https://www.smithsonianmag.com/smart-news/fisa-court-has-only-denied-nsa-request-once-past-5-years-180951313/.

99 Dominic Rushe, *Yahoo $250,000 Daily Fine over NSA Data Refusal Was Set to Double 'Every Week'*, GUARDIAN (Sept. 12, 2014, 5:33 PM), http://www.theguardian.com/world/2014/sep/11/yahoo-nsa-lawsuit-documents-fine-user-data-refusal.

should adapt.

B. Scholarly Criticism

Former Google CEO Eric Schmidt once remarked: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[100] The concern of the Fourth Amendment is not to give people space to do things they "shouldn't be doing." Rather, the concern is to allow people to live core areas of their personal lives with the dignity that excludes onlookers.[101] It is to permit people space to do those unpopular or disfavored things which authorities *merely think* people "shouldn't be doing." When the government intrudes on this space, it risks sliding into the sort of totalitarianism that the United States spent forty-five years resisting. In the words of Justice William O. Douglas:

> When an intelligence officer looks over every nonconformist's shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the image which Jefferson and Madison designed, but more in the Russian image . . . .[102]

As Justice Sotomayor has recently observed, Fourth Amendment protections are also crucial to ensuring the exercise of other constitutional guarantees: "Awareness that the Government may be watching chills associational and expressive freedoms."[103] People share information with third parties all the time—the colleagues, friends, and corporations they interact with on a daily basis. That is a social and economic necessity. But when those with the power to punish have access to that same information, the stakes change.[104] The power to punish is the power to suppress messages and identities that are unpopular or perceived to be threatening. The disfavored messages and

---

100 *Google CEO on Privacy (VIDEO): 'If You Have Something You Don't Want Anyone to Know, Maybe You Shouldn't Be Doing It'*, HUFFINGTON POST (Mar. 18, 2010, 5:12 AM), https://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html (last updated Dec. 6, 2017).

101 *See* John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 664, 681 (explaining that while privacy is the overarching rationale behind the Fourth Amendment's requirement of reasonable searches, "[t]he Court . . . has intermittently cited the protection of human dignity as a concern under the Fourth Amendment").

102 Laird v. Tatum, 408 U.S. 1, 28–29 (1972) (Douglas, J., dissenting).

103 United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

104 ROBERT SCHEER, THEY KNOW EVERYTHING ABOUT YOU: HOW DATA-COLLECTING CORPORATIONS AND SNOOPING GOVERNMENT AGENCIES ARE DESTROYING DEMOCRACY 14 (2015) ("It is one thing to have a private company mine your data for better leads on shopping or viewing but quite another for your government to be doing that snooping . . . .").

identities of one day are the seeds of social progress for the next.[105]

Scholars have proposed different ways of resolving the tension between the Fourth Amendment and the third-party doctrine in the present day. One solution could be to abandon or severely limit the third-party doctrine.[106] However, the Court is unlikely to set aside over forty years of third-party jurisprudence.[107] Not only are judicial habits hard to break, but the third-party doctrine often makes sense and has a crucial role to play in keeping us safe. The Fourth Amendment is a balance of interests between protecting privacy and providing authorities with the information they need to protect the public.[108] When authorities have less information, they are less able to prevent crime and its harmful consequences.[109] That safety mission should be compromised only when there are counterbalancing interests that outweigh those of future victims. The third-party doctrine appropriately identifies some scenarios where those counterbalancing interests are weak or non-existent. Sharing something during a loud conversation on the subway or to hundreds of friends on Facebook suggests that the dignity interests that may otherwise attach to that information are weak or have been voluntarily forfeited.[110] Similarly, the concerns about chilled speech or association that Justices Douglas and Sotomayor raised are less immediate for parties who

---

105 *See* Lyman Abbott, *Why Women Do Not Wish the Suffrage*, ATLANTIC (Sept. 1903), https://www.theatlantic.com/magazine/archive/1903/09/why-women-do-not-wish-the-suffrage/306616/ ("In 1895 the women of Massachusetts were asked by the state whether they wished the suffrage. Of the 575,000 voting women in the state, only 22,204 cared for it enough to deposit in a ballot box an affirmative answer to this question. That is, in round numbers, less than four per cent wished to vote; about ninety-six per cent were opposed to woman suffrage or indifferent to it. That this expresses fairly well the average sentiment throughout the country can hardly be questioned.").

106 Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 84 (2011) ("[T]he third-party doctrine of the Fourth Amendment has come to a breaking point . . . ."); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 268 (2016) ("[A]pplying the third-party rule in today's world is inconsistent with the history and purpose of the Fourth Amendment.").

107 A version of the third-party doctrine first entered Fourth Amendment jurisprudence in 1976. Price, *supra* note 106, at 264 ("The 'third-party doctrine' originated with two Supreme Court decisions in the late 1970s, *United States v. Miller* and *Smith v. Maryland*.").

108 *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2484–85 (2014) (balancing the government and privacy interests in deciding whether to apply the Fourth Amendment's search incident to arrest exception to cell phones).

109 Kerr, *supra* note 22, at 573.

110 *See* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (explaining Mark Zuckerberg's view that people have become comfortable making all sorts of previously private personal information public).

feel safe speaking and associating openly.[111]

A different approach that some scholars prefer would be to patch the doctrine from the outside by using legislation to require third-party service providers to be more transparent to consumers about what will and could happen with their data.[112] Europe, for example, has much more demanding data transparency laws.[113] The Department of Commerce runs a program that registers United States companies as "Safe Harbor Compliant," meaning that their data-use policies satisfy European Union requirements.[114] More data transparency in the United States would certainly be an improvement, but it is doubtful that would help with the concerns raised here. It could educate users about the current legal implications of using third-party services,[115] but for that to make a difference, people need to have a real alternative to sharing their information. Modern social and economic realities leave people no choice but to make use of the third-party services providers that assist their phones, laptops, and watches.[116] Those with

---

111 *See* Mary Madden et al., *Teens, Social Media, and Privacy*, PEW RES. CTR. (May 21, 2013), http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/ ("Teen social media users do not express a high level of concern about third-party access to their data . . . .").

112 *See* Mary Graw Leary, *The Missed Opportunity of* United States v. Jones*: Commercial Erosion of Fourth Amendment Protection in a Post Google Earth World*, 15 U. PA. J. CONST. L. 331, 334 (2012) ("This Article proposes a new legislative framework for respecting privacy protections in response to these commercial-induced privacy affronts. This framework, supported by analogous American law and European proposals, calls for an opt-in model: before an individual can be assumed to have voluntarily sacrificed his privacy, he must affirmatively opt in to allow the use of his private data. The opt-in must, however, be meaningful and not an unfair component of a terms of service agreement.").

113 *See The OECD Privacy Framework*, OECD (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf ("Openness Principle . . . There should be a general policy of openness about developments, practices and policies with respect to personal data.").

114 *See Search the U.S.-EU Safe Harbor List*, EXPORT.GOV, https://www.export.gov/safeharbor_eu (last visited Feb. 24, 2018); *see also* Letter from Penny Pritzker, Sec'y of Commerce, U.S. Dep't of Commerce, to Vera Jourová, Comm'r for Justice, Consumers and Gender Equal., European Comm'n (Feb. 23, 2016), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf; Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Vera Jourová, Comm'r for Justice, Consumers and Gender Equal., European Comm'n (Feb. 23, 2016), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

115 Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, CONVERSATION (May 29, 2017, 9:48 PM), https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404 ("Transparency, education and strong regulatory frameworks are the key. Users need to know what information about them is being collected, by whom, and what it's being used for. Only then can we as a society decide what privacy protections are appropriate, and put them in place. Our findings, and those of many other researchers, can help turn the tables and track the trackers themselves.").

116 *Id.*; *see also* Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1929 (2017) [hereinafter *If These Walls Could Talk*] ("[I]t's not clear that our modern consistent conveyance of personal information to third parties is . . .

sufficient resources[117] can pay for premium privacy-protective services that function without access to customer data—like Riseup[118] for email or SpiderOak[119] for cloud storage. But relying on for-pay services risks making privacy a privilege for the privileged. "[T]he Constitution doesn't prefer the rich over the poor . . . ."[120]

More promising proposals for addressing the overreach of the third-party doctrine work from within. One such approach focuses on the notion of consent.[121] The third-party doctrine only applies to information that has been "voluntarily" turned over to third parties.[122] Most third-party service

---

voluntary . . . . Increasingly, disclosure of such information is necessary to participate in modern life."); Ghoshray, *supra* note 106, at 74–75 ("This voluntary-involuntary distinction falls flat on its face when confronted with the stark reality that the post-modern individual conducts life through the enabling means of the Internet and may, indeed, have a fundamental right to Internet access.").

117 *See, e.g.*, Matt Sledge, *Alex Kozinski, Federal Judge, Would Pay $2,400 a Year, Max, for Privacy*, HUFFINGTON POST (March 4, 2013, 5:51 PM), http://www.huffingtonpost.com/2013/03/04/alex-kozinski-privacy_n_2807608.html. *See generally* JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014).

118 *See About Us*, RISEUP, https://riseup.net/en/about-us (last visited Feb. 24, 2018) ("Can you rely on a corporate email provider for confidentiality of your sensitive email communications? Not only do they typically scan and record the content of your messages for a wide variety of purposes, they also concede to the demands of governments that restrict digital freedom and fail to have strict policies regarding their user's privacy.").

119 *See The SpiderOak Collaboration Suite*, SPIDEROAK, https://spideroak.com/ (last visited Feb. 24, 2018) ("For over 10 years, SpiderOak has built software based on a singular, unwavering belief: that the world is a better place if software is trustworthy and secure. SpiderOak software allows you to communicate, collaborate, and organize within the confines of the most restrictive compliance regulations.").

120 United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, C.J., dissenting).

121 See Mary Graw Leary, Katz *on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 374 (2013) ("By reinvigorating voluntariness into the search jurisprudence and the Third Party doctrine, this proposal suggests only a minor adjustment in current law."); *see also If These Walls Could Talk*, *supra* note 116, at 1925; Leary, *supra* note 112, at 334.

122 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973) ("[T]he question whether a consent to a search was in fact 'voluntary' or was the product of duress or coercion, express or implied, is a question of fact to be determined from the totality of all the circumstances. While knowledge of the right to refuse consent is one factor to be taken into account, the government need not establish such knowledge as the *sine qua non* of an effective consent. As with police questioning, two competing concerns must be accommodated in determining the meaning of a 'voluntary' consent—the legitimate need for such searches and the equally important requirement of assuring the absence of coercion."); *In re* Application of the United States, 830 F. Supp. 2d 114, 133 (E.D. Va. 2011) *(*"Even if Petitioners had a reasonable expectation of privacy in IP address information collected by Twitter, Petitioners voluntarily relinquished any reasonable expectation of privacy under the third-party doctrine. To access Twitter, Petitioners had to disclose their IP addresses to third parties. This voluntary disclosure—built directly into the architecture of the Internet—has significant Fourth Amendment consequences under the third-party doctrine, as articulated in *United States v. Miller* and *Smith v. Maryland*.").

providers ask users to click "I Agree" to some sort of privacy disclosure.[123] But the average person cannot understand the legalese in which these are usually written.[124] Even if she can understand which information she is sharing, fully appreciating the significance of doing so requires some background in data science.[125] "Anonymous location data" (which many privacy policies say service providers collect) sounds like it protects a person's identity. Yet, as data researchers have shown, it does not—just four "anonymous" date/location points will identify a person with ninety-five percent accuracy.[126] Are people really consenting to turn over their information when they do not understand what information that is or the implications of doing so? Some of the data transparency initiatives discussed above may help address this consent concern, but, once again, only if people have alternatives to agreeing to the data policies of the third-party service providers. The other side of the worry with the consent argument is that it risks proving too much. If people never really consent when they click "I Agree," the third-party doctrine will be severely compromised, and the ability of authorities to protect us along with it.

A different kind of argument, again working within the framework of the third-party doctrine, may help rein in the doctrine for some service

---

123 *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274, 87,275 (Dec. 2, 2016) (to be codified at 7 C.F.R. pt. 64) ("We adopt rules requiring carriers to obtain customers' opt-in approval for use and sharing of sensitive customer PI (and for material retroactive changes to carriers' privacy policies). A familiar example of opt-in practices appears when a mobile application asks for permission to use geo-location information.").

124 *See* Alex Kozinski & Mihailis E. Diamantis, *An Eerie Feeling of Déjà Vu: From Soviet Snitches to Angry Birds*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 425 (David Gray & Stephen E. Henderson eds., 2017) ("The privacy agreements are written by lawyers and techies, for lawyers and techies, usually with no effort to make them penetrable to the vast majority of users."); Umika Pidaparthy, *What You Should Know About iTunes' 56-Page Legal Terms*, CNN (May 6, 2011, 7:08 AM), http://www.cnn.com/2011/TECH/web/05/06/itunes.terms/index.html (noting the opinion of technology attorney Mark Grossman that "[m]ost people really just don't understand digital rights management"); *see also* David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, GUARDIAN (Mar. 3, 2017, 8:38 AM), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print ("Only a quarter of the 543 students even bothered to look at the fine print. But 'look' is not 'read': on average, these more careful joiners spent around a minute with the thousands of words that make up NameDrop's privacy and service agreements. And then they all agreed to them.").

125 *See* Kozinski & Diamantis, *supra* note 124, at 425 ("Suppose you are a lawyer with the extraordinary patience to read a privacy agreement. You may understand what you've agreed to formally. But unless you know a good deal about big data science, you probably have no idea what you've *really* agreed to. The app developers, and whomever else they sell your data to, will know the information you've allowed them to collect, but also everything they can infer from aggregating all the information. Those inferences are the most valuable part.").

126 *See* Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, NATURE (Mar. 25, 2013), http://www.nature.com/articles/srep01376.

providers.[127] Recall that the third-party doctrine does not apply when the third party is an instrument of state, acting with too much direction or encouragement from the government.[128] Courts consider two factors when determining whether a third party is an instrument of state: 1) the degree of government involvement, knowledge, and acquiescence, and 2) the intent of the party conducting the search.[129] Some third-party service providers satisfy these factors quite nicely because the government's level of involvement, knowledge, and acquiescence in collecting that data is extremely high. Consider, for example, cell companies that log user geolocation data. On the front end, the federal government requires cell companies to do this for 911 emergency response purposes.[130] Then, on the back end, the government purchases the location data the cell companies collect.[131] The government is involved, albeit not directly, throughout the process. This makes cell companies, at least so far as customer geolocation is concerned, seem a lot like instruments of state rather than third parties. In other cases, though, the factors will not so clearly mark a third-party service provider as an instrument of state. Most will likely fall in the "gray area" of all balancing tests and require individualized consideration.[132] A more sweeping fix would be preferable.

A final approach to fixing the third-party doctrine, and the approach adopted by this Article, is to ask whether the Supreme Court has an adequate understanding of "privacy," the reasonable expectation of which the Fourth Amendment protects. As argued above, the Supreme Court's implicit conception of privacy is as a kind of secrecy. That is the best explanation of why the third-party doctrine has been given such a long reach—secrets told to third parties are secrets no more. Other scholars have recognized that there are different understandings of privacy and that the Court's is unnecessarily restrictive.[133] Things we share with our spouses, friends, and doctors are private, even if they are no longer totally secret. What is needed is an alternate theory.

---

127 *See* Kozinski & Diamantis, *supra* note 124, at 436 ("The infrastructure for a potential surveillance state is in place, and it is largely in private hands. . . . The third-party doctrine, which currently gives the government easy access to any information that passes through the private infrastructure, is dangerously outdated. We . . . suggest[ ] . . . treating many corporations with access to customer data as instruments of state.").

128 *See id.* at 433.

129 United Sates v. Walther, 652 F.2d 788, 792 (9th Cir. 1981).

130 *See Fact Sheet: FCC Wireless 911 Requirements*, *supra* note 76.

131 *See* Kozinski & Diamantis, *supra* note 124, at 424 ("Data brokers make good money when the government buys data that would cost much more to acquire itself.").

132 *Walther*, 652 F.2d at 791.

133 *See* SCHULHOFER, *supra* note 23, at 8 ("The idea that privacy means secrecy is too narrow even when we think only about personal information . . . .").

Stephen J. Schulhofer suggests that privacy is about having control over our information rather than keeping it secret.[134] This seems like a step in the right direction. Schulhofer's conception of privacy recognizes that people can share information with third parties in ways that nonetheless maintain its privacy.[135] He argues that his privacy-as-control approach would require the government to get a warrant for customer data held by service providers when customers have no realistic alternative but to provide their information.[136] So far so good. But Schulhofer's proposal is unlikely to get Supreme Court buy-in. It is an entirely new theory of privacy. While the Court does sometimes make dramatic pivots in doctrine, it tends to prefer incremental change built on familiarity.[137] Since Schulhofer's approach has no precedent in law, its boundaries and implications are difficult to anticipate. For example, what happens in cases where control and privacy seem to come apart, as when someone tells everyone but a single frenemy about an upcoming party? This seems like a situation that involves meticulous control over information, but no intuitive privacy interest deserving constitutional protection.

The Court would be more likely to accept a more familiar and well-litigated notion of privacy, with established contours and implications. It is to this that the Article now turns.

II. ATTORNEY-CLIENT CONFIDENCES

Fourth Amendment jurisprudence is not the only area of law where the concept of privacy has an important role to play. Tort law recognizes a cause of action for invasion of privacy.[138] Statutory schemes like the Health Insurance Portability and Accountability Act[139] and the Family Educational Rights and Privacy Act[140] direct custodians of certain private information to

134 *Id.* at 8–9.

135 *Id.*

136 *Id.* at 140–42.

137 *See generally* Lisa A. Kloppenberg, *Measured Constitutional Steps*, 71 IND. L.J. 297 (1996) (discussing the tendency of courts to rule narrowly with incremental changes to doctrine, as opposed to broadly with drastic changes to doctrine).

138 RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST., 1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

139 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1177, 110 Stat. 1936, 2029 (1996) (detailing the offense and penalties of wrongful disclosure of individually identifiable health information).

140 Family Education Rights and Privacy Act, 20 U.S.C. § 1232(g)(b)(1)(L) (2012) (describing the

prevent outside access. And common law evidentiary privileges protect some private information from discovery, whether by opposing parties or by the government.[141] It is surprising that Fourth Amendment privacy scholars have underappreciated these reserves of insight into what privacy is and can be. Evidentiary privilege should be a particularly appealing resource because it can serve to protect information from the government, even in the face of a duly issued search warrant.[142] Focusing on attorney-client privilege, this Part starts to unpack the potential benefits of such doctrinal cross-pollination.

A. Background to the Attorney-Client Privilege

Attorney-client privilege is a common law doctrine that applies in state and federal courts alike.[143] Among common law privileges, it is the oldest.[144] It emerged in England nearly five hundred years ago as part of the law of witnesses.[145] The jury trial was just starting to replace outmoded practices like trial by ordeal or combat,[146] which sought to channel divine judgment

---

importance of an agency caseworker or other representative of a State and local child welfare agency not disclosing a student's case plan).

141 United States v. Bryan, 339 U.S. 323, 331–32 (1950) ("'[T]he public . . . has a right to every man's evidence. When we come to examine the various claims of exemption, we start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional . . . .' Every exemption from testifying or producing records thus presupposes a very real interest to be protected. If a privilege based upon that interest is asserted, its validity must be assessed." (footnote omitted)); *see also* Jaffee v. Redmond, 518 U.S. 1, 13–14 (1996) (discussing patient-therapist privilege); Trammel v. United States, 455 U.S. 40, 41–42 (1980) (discussing spousal privilege); *In re* Grand Jury Investigation, 918 F.2d 374, 384–85 (3d Cir. 1990) (discussing confessional privilege).

142 *See* United States v. Taylor, 764 F. Supp. 2d 230, 236 (D. Me. 2011) (showing that the government must use a filtering agent to cull out potentially privileged information before reviewing emails obtained pursuant to a search warrant); Nat'l City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980) ("[A] law office search should be executed with special care to avoid unnecessary intrusion on attorney-client communications . . . ."); U.S. DEP'T OF JUSTICE, U.S. ATT'Y MANUAL § 9-13.420(E) ("[E]very effort should be made to avoid viewing privileged material [during a search]."); Eric D. McArthur, *The Search and Seizure of Privileged Attorney-Client Communications*, 72 U. CHI. L. REV. 729, 756 (2005) ("[P]rivileged attorney-client communications cannot be searched and seized.").

143 FED. R. EVID. 501 ("The common law—as interpreted by the United States courts in light of reason and experience—governs a claim of privilege . . . .").

144 Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

145 1 PAUL R. RICE ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES § 1:2 (2017), Westlaw; *see also* CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, 2 FEDERAL EVIDENCE § 5:13, at n.1 (4th ed.), Westlaw (database updated June 2018) [hereinafter FEDERAL EVIDENCE] (citing Berd v. Lovelace (1577) 21 Eng. Rep. 33; Cary 62; Dennis v. Codrington (1580) 21 Eng. Rep. 53; Cary 100).

146 RICE ET AL., *supra* note 145.

through harrowing feats.[147] Without access to a Judge on high to render verdicts, courts needed human witnesses to testify about the facts during trial. Parliament responded by passing the Statute Against Perjury in 1562,[148] which enabled courts to compel witnesses to testify. Because the law at the time did not permit parties to testify in their own cases, litigants instead sought to compel testimony from their opponents' lawyers.[149] The first attorney-client privilege cases emerged soon after to address the obvious problems this dynamic raised.[150]

The justification common law courts gave for the privilege shifted about over the centuries. Originally, the stated purpose behind the doctrine was to protect attorneys' honor, since they were duty-bound to keep client confidences.[151] As a consequence, courts originally ruled that it was the attorney rather than the client who held and controlled the privilege.[152] Society and attorneys clearly understood that revealing a client's confidences would be an act of betrayal[153] at which "[e]very feeling of justice, honour and humanity[ ] would be shocked."[154] Thus, at their core, such "humanistic"

147 Trisha Olson, *Of Enchantment: The Passing of the Ordeals and the Rise of the Jury Trial*, 50 SYRACUSE L. REV. 109, 117 (2000) ("The proofs cited most routinely are the ordeal of the iron, which consisted of a proband carrying a red-hot iron for a specified distance, and the ordeal of the cauldron, which required him to pluck an object from boiling water. An affirmative judgment required that the wound heal cleanly within three days time." (footnotes omitted) (citing ROBERT BARTLETT, TRIAL BY FIRE AND WATER 13–22 (1986); then citing R.S. VAN CAENEGEM, LEGAL HISTORY: A EUROPEAN PERSPECTIVE 75–76 (1991))).

148 *See Developments in the Law: Privileged Communications*, 98 HARV. L. REV. 1450, 1455 n.9 (1985) (noting that the Statute Against Perjury imposed a "universal duty" on witnesses to testify when called upon).

149 *See* RICE ET AL., *supra* note 145.

150 *Id.*; *see also* Austen v. Vesey (1577) 21 Eng. Rep. 34, 34; Cary 63, 63; Berd v. Lovelace (1577) 21 Eng. Rep. 33, 33; Cary 62, 62 ("Thomas Hawtry, gentleman, was served with a subpoena to testify his knowledge touching the cause in variance; and made oath that he bath been, and yet is a solicitor in this suit, and hath received several fees of the defendant; which being informed to the Master of the Rolls, it is ordered that the said Thomas Hawtry shall not be compelled to be deposed, touching the same, and that he shall be in no danger of any contempt, touching the not executing of the said process . . . .").

151 *See* Anonymus (1694) 90 Eng. Rep. 179, 179–80; Skinner 404, 404 ("In a trial at Nisi Prius in Westminster, one Saunders an attorney who had drawn an indenture of agreement between a sheriff and his under-sheriff, being produced to prove a corrupt agreement between them; he was not compelled to discover the matter of it, though he was not a counsellor; and per Holt Chief Justice, it seems to be the same law of a scrivener; and he cited a case where upon a covenant to convey as counsel shall advise, & consilium non dedit advisamentum being pleaded, conveyances made by the advice of a scrivener being tendred and refused, was allowed to be good evidence upon this issue; for he is a counsel to a man, with whom he will advise; if he be instructed and educated in such way of practice, otherwise of a gentleman, parson . . . .").

152 *Id.*

153 1 EDWARD J. IMWINKELRIED & EDWARD L. BARRETT, JR., THE NEW WIGMORE: A TREATISE ON EVIDENCE § 2.3, at 169–71 (Richard D. Friedman & Ralph W. Aigler eds., 3d ed. 2017).

154 EDWARD LIVINGSTON, THE COMPLETE WORKS OF EDWARD LIVINGSTON ON CRIMINAL

justifications for the attorney-client privilege sought to prevent attorneys from becoming "potential adversaries who could be pitted against the people they seek to serve."[155]

During the eighteenth century, the focus shifted from attorneys' interests in honor to clients' interests in effective counsel. As one judge put it:

> [T]he interest which [the client] has in this privilege, is very obvious. No man can conduct any of his affairs which relate to matters of law, without employing and consulting with an attorney . . . and if he does not fully and candidly disclose every thing that is in his mind, which he apprehends may be in the least relative to the affair he consults his attorney upon, it will be impossible for the attorney properly to serve him . . . .[156]

With this development arose the rule that the clients control the privilege, and only they (not their attorneys) can waive it. [157]

Until the nineteenth century, attorney-client privilege applied to a relatively limited range of attorney-client communications—those providing advice in anticipation of litigation.[158] In 1833, common law courts removed this restriction in one of the most important attorney-client privilege cases, *Greenough v. Gaskell*.[159] The issue in *Gaskell* was whether a client could claim the privilege over accounts and letters prepared, dictated, or received by an attorney "in his character or situation of confidential solicitor to the [client]."[160] The court opined that:

> [I]t does not appear that the protection is qualified by any reference to proceedings pending or in contemplation. If touching matters that come within the ordinary scope of professional employment, they [attorneys] receive a communication . . . from a client . . . they are not only justified in withholding such matters, but bound to withhold them, and will not be compelled to disclose the information or produce the papers in any Court of law or equity, either as party or as witness. If this protection were confined to cases where proceedings had commenced, the rule would exclude the most confidential, and it may be the most important of all communications—those made with a view of being prepared either for

---

JURISPRUDENCE; CONSISTING OF SYSTEMS OF PENAL LAW FOR THE STATE OF LOUISIANA AND FOR THE UNITED STATES OF AMERICA 461 (1873).

155 FEDERAL EVIDENCE, *supra* note 145, § 5:13.

156 Annesley v. Earl of Anglesea, 17 How. St. Tr. 1139, 1237 (Ex. 1743).

157 Lord Say & Seal's Case (1712) 88 Eng. Rep. 617, 617; 10 Mod. 40, 41 ("The Court were of opinion, that *Holbeche's case* was good law; and that an attorney's privilege was the privilege of his client . . . .").

158 RICE ET AL., *supra* note 145, §§ 1:6–9. Some historians have argued that the privilege only extended to barristers, but a close look at the cases reveals that communications with other attorneys were also privileged when they were in anticipation of litigation. Barristers were simply the attorneys whose clients were most likely to communicate with in anticipation of litigation. *See id.*; Berd v. Lovelace (1577) 21 Eng. Rep. 33, 33; Cary 62, 62.

159 (1833) 39 Eng. Rep. 618; 1 My. & K. 98.

160 *Id.* at 620.

> instituting or defending a suit, up to the instant that the process of the Court issued.[161]

This was the start of the expansive scope of the attorney-client privilege familiar today. Thus, by 1873, a court could write:

> [I]t is not now necessary as it formerly was, for the purpose of obtaining production, that the communications should be made either during or relating to an action or even to an expected litigation. It is sufficient if they pass as professional communications [with an attorney] in a professional capacity.[162]

American courts imported this law of attorney-client privilege from England with very little change.[163] First recognized by the Supreme Court in 1826,[164] the privilege has been employed to serve "broader public interests in the observance of law and administration of justice."[165] American courts tended to see the privilege in purely instrumental terms, as an essential "means to the end of promoting certain desirable social consequences."[166] The privilege helps people stay informed about what the law requires of them by facilitating full and frank discussion between attorneys and the clients seeking their advice. A client who cannot be sure that all statements to her attorney would be safe from discovery and exploitation by an opposing party may choose not to seek legal advice or not to disclose all important information.[167]

That instrumental rationale is still the prevailing justification for the attorney-client privilege today.[168] Although the precise elements of the

---

161 *Id.*

162 Lawrence v. Campbell (1859) 62 Eng. Rep. 186, 188; 4 Drewry 485, 490.

163 *See, e.g.*, Parker v. Carter, 18 Va. 273, 286 (1814) ("[C]ounsel and attornies ought not to be permitted to give evidence of facts imparted to them, by their clients, when acting in their professional character; that they are considered as identified with their clients, and, of necessity, entrusted with their secrets, which, therefore, without a dangerous breach of confidence, cannot be revealed; that this obligation of secrecy continues always, and is the privilege of the client, and not of the attorney. The court is also of opinion, that this restriction is not confined to facts disclosed, in relation to suits actually depending at the time, but extends to all cases in which a client applies, as aforesaid, to his counsel or attorney, for his aid in the line of his profession.").

164 *See* Chirac v. Reinicker, 24 U.S. 280, 294 (1826) ("The general rule is not disputed, that confidential communications between client and attorney, are not to be revealed at any time.").

165 Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

166 IMWINKELRIED & BARRETT, *supra* note 153, § 2.4, at 174–75; *see also Upjohn*, 449 U.S. at 389 ("[The privilege's] purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.").

167 FEDERAL EVIDENCE, *supra* note 145, § 5:13.; IMWINKELRIED & BARRETT, *supra* note 153, § 2.4, at 174–75.

168 FEDERAL EVIDENCE, *supra* note 145, § 5:13.

attorney-client privilege vary among jurisdictions, Professor Wigmore's definition is a common model:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[169]

Accordingly, the attorney-client relationship begins when a prospective client approaches an attorney with the intent of receiving the attorney's services and legal advice.[170] The privilege attaches to all initial interview communications before that point, regardless of whether representation is offered or declined, and then to all confidential communications once the offer for representation is accepted.[171] Thus, as long as a client can provide sufficient evidence to meet each of the above elements the attorney-client privilege will apply. Once the relationship is created, the duration of the privilege is indefinite, even lasting beyond a client's death, unless it is waived beforehand.[172]

B. Confidentiality and Third Parties

Though the attorney-client privilege is often referred to as an "absolute" privilege, there are conditions in which courts will hold that the privilege, and its protections, have been waived.[173] The focus of the waiver inquiry is the fourth element in Wigmore's definition of the privilege—confidentiality.[174] If attorney-client communications lose their confidential

---

169 WIGMORE, *supra* note 25, at 554 (emphasis omitted).

170 RICE ET AL., *supra* note 145, § 2:4.

171 *Id.*

172 Swidler & Berlin v. United States, 524 U.S. 399, 406–07 (1998).

173 RICE ET AL., *supra* note 145, § 2:2.

174 WIGMORE, *supra* note 25, § 2292, at 554; *see* IMWINKELRIED & BARRETT, *supra* note 153, § 6.12.2, at 1155–56 (discussing that the burden of proof in waiver cases revolves around a privilege holder showing that the initial communication was confidential and that confidentiality has been maintained); *see also* Hartford Fire Ins. Co. v. Garvey, 109 F.R.D. 323, 327 (N.D. Cal. 1985) ("The confidentiality element and waiver are closely related inasmuch as any voluntary disclosure inconsistent with the confidential nature of the attorney client relationship waives the privilege."). There are other ways clients can waive the privilege that do not implicate confidentiality. For example, if a client asserts an advice of counsel defense in a criminal trial, or otherwise refers to the contents of attorney-client communications to disadvantage their opponents. Rhone-Poulenc Rorer Inc. v. Home Indem. Co., 32 F.3d 851, 863 (3d Cir. 1994) ("A defendant may also waive the privilege by asserting reliance on the advice of counsel as an affirmative defense." (citing cases)); *see also* BARBARA J. VAN ARSDALE ET AL., 81 AMERICAN JURISPRUDENCE: WITNESSES § 329 (2d ed. 2018), Westlaw ("[A] party waives the attorney-client privilege by placing the advice of counsel in issue only where the client asserts the claim or defense and attempts to prove that claim or defense

nature, they are no longer privileged.

The confidentiality requirement was an early American addition to the common law of attorney-client privilege.[175] Over the course of the twentieth century, the confidentiality requirement became the majority rule in U.S. jurisdictions.[176] The private-public interest balancing rationale behind the development is strikingly similar to the rationale behind the warrant requirement of the Fourth Amendment. The interest in encouraging clients to be forthcoming with their attorneys must be balanced against the interests adverse parties (including government authorities) have in gathering all available evidence.[177] Clients who are unconcerned about confidentiality do not need the protections of the privilege to coax them to seek legal advice.[178] Consequently, in such cases the balance of interests tips in favor of evidentiary transparency, and against the privilege.

The standards courts use to measure confidentiality are also structurally reminiscent of Fourth Amendment doctrine. Recall that the warrant requirement attaches to information in which a person has a reasonable expectation of privacy, as measured by subjective and objective criteria.[179] Similarly, for an attorney-client communication to be considered confidential, the client must subjectively intend that the communications to the attorney are confidential, and such intent must be objectively reasonable under the circumstances.[180] The communications must be confidential when first conveyed, and confidentiality must be maintained at all times afterwards.[181]

---

by disclosing or describing an attorney-client communication . . . ."). These modes of waiver serve as practical exceptions to the general rule that confidential attorney communications are privileged, because any other rule would unfairly allow parties to use the privilege "both as a sword and shield" against opposing parties. Rock River Commc'ns, Inc. v. Universal Music Grp., Inc., 745 F.3d 343, 353 (9th Cir. 2014) (quoting Chevron Corp. v Pennzoil Co., 974 F.2d 1156, 1162 (9th Cir. 1992)).

175 RICE ET AL., *supra* note 145, at § 6:3. Early U.S. cases held that attorneys could not be compelled to testify to non-confidential communications, though third parties aware of the communication could be. *Id.* (citing Jackson v. French, 3 Wend. 337 (N.Y. Sup. Ct. 1829)).

176 *Id.*

177 Charles W. Wolfram, *The U.S. Law of Client Confidentiality: Framework for an International Perspective*, 15 FORDHAM INT'L L.J. 529, 544 (1991).

178 *See* Paul R. Rice, *Attorney-Client Privilege: The Eroding Concept of Confidentiality Should Be Abolished*, 47 DUKE L.J. 853, 859 (1998) (explaining that "the protection of the privilege is not 'necessary to secure the client's subjective freedom of consultation'" when the client freely chooses to communicate in certain situations, such as when a third party is present (footnote omitted)).

179 *See supra* Section I.A.

180 RICE ET AL., *supra* note 145, § 6:1; *see, e.g.*, United States v. Dennis, 843 F.2d 652, 657 (2d Cir. 1988) ("The key, of course, to whether an attorney/client relationship existed is the *intent* of the client and whether he *reasonably* understood the conference to be confidential." (emphasis added)).

181 *See, e.g.*, United States v. Pipkins, 528 F.2d 559, 563 (5th Cir. 1976) ("It is vital to a claim of privilege

As with privacy under the Fourth Amendment, the concept of confidentiality in the law of privilege is best defined by its breach. Clients are said to "waive" the privilege, whether intentionally or not, when they do something that compromises the confidentiality of the privileged information. This is where the attorney-client privilege's version of the third-party doctrine comes in. Disclosure of privileged information to a third party may[182] "destroy[] both the communications' confidentiality and the privilege that is premised upon it."[183] Courts reason that a client who allows third parties to overhear or otherwise access communications to her attorney cannot intend those communications to be confidential.[184] Even unintentional disclosure to a third party may waive the privilege.[185]

Privilege waiver, however, differs in two crucial respects from the Fourth Amendment's third-party doctrine that give the former a lighter, more nuanced touch. To begin, the circle of third parties to whom information can be revealed without shedding its confidential character is much wider.[186] The only parties formally excepted from the third-party doctrine are instruments of state—a person's reasonable expectation of Fourth Amendment privacy is not undermined if the third party is acting at the direction of the government.[187] The law of privilege, however, must be different—its very existence is premised on the presence of a third party (the attorney). It recognizes that there are many contexts where communications with third parties are confidential and many important relationships that would be undermined if evidentiary privileges did not apply, such as

---

that the communication have been made and maintained in confidence.").

182 *See* Upjohn Co. v. United States, 449 US 383, 396 (1981) ("[T]he recognition of a privilege based on a confidential relationship . . . should be determined on a case-by-case basis." (alteration in original) (internal quotation marks omitted) (quoting S. REP. NO. 93-1277, at 17 (1974)).

183 RICE ET AL., *supra* note 145, § 9:29 (citing United States v. Arthur Young & Co., 465 U.S. 805, 819 (1984)).

184 Frank v. Morley's Estate, 64 N.W. 577, 578 (Mich. 1895) ("The communication was not made in any confidence which excluded [another individual], . . . and under such circumstances the privilege does not exist.").

185 *Compare* Dion Messer, *To: Client@Workplace.com: Privilege at Risk?*, 23 J. MARSHALL J. INFO. TECH. & PRIVACY L. 75, 93–95 (2004) (discussing cases where inadvertent disclosure resulted in waiver), *with* FED. R. EVID. 502(b) (outlining circumstances where inadvertent disclosure in the federal setting will not result in waiver).

186 Georgia v. Randolph, 547 U.S. 103, 133 (2006).

187 *See supra* notes 42–43 and accompanying text.

spousal,[188] medical,[189] psychiatric,[190] and confessional relationships.[191] These relationships form a network of third parties linked by a commitment to confidentiality; they often require that information be shared between them.[192]

A person worrying about past misdeeds may need to tell her attorney and her priest the same stories. A person's legal troubles may be the source of her psychiatric angst. And her spouse may be just as important a source of support and advice as her attorney during legal conflict. Forcing a waiver of attorney-client privilege when a client shares attorney-client communications to third parties in these relationships would undermine not only the value those relationships offer, but also the attorney-client relationship.[193] The law recognizes this fact and does not hold that disclosure of attorney-client communications to one's spouse, doctor, psychiatrist, or priest undermines confidentiality.[194]

---

188 Wolfle v. United States, 291 U.S. 7, 14 (1934) ("The basis of the immunity given to communications between husband and wife is the protection of marital confidences, regarded as so essential to the preservation of the marriage relationship as to outweigh the disadvantages to the administration of justice which the privilege entails. . . . Communications between the spouses, privately made, are generally assumed to have been intended to be confidential, and hence they are privileged; but wherever a communication, because of its nature or the circumstances under which it was made, was obviously not intended to be confidential it is not a privileged communication." (internal citations omitted)); *see also* Trammel v. United States, 445 U.S. 40, 51–52 (1980) (recognizing the distinction between the privilege protecting spousal communications and rights regarding the spousal testimonial privilege in trials and eventually concluding that the witness spouse alone holds the testimonial privilege and may waive it in order to testify adversely to his or her spouse).

189 People v. Al-Kanani, 307 N.E.2d 43, 44 (N.Y. 1973) (noting that New York was the first state to statutorily recognize the physician-client privilege, which was not recognized at common law, because the privilege "protect[s] those who are required to consult physicians from the disclosure of secrets imparted to them, to protect the relationship of patient and physician and to prevent physicians from disclosing information which might result in humiliation, embarrassment, or disgrace to patients" (internal quotation marks omitted) (quoting Steinberg v. N.Y. Life Ins. Co., 188 N.E. 152, 153 (N.Y. 1933))).

190 Jaffee v. Redmond, 518 U.S. 1, 10 (1996) ("Like the spousal and attorney-client privileges, the psychotherapist-patient privilege is 'rooted in the imperative need for confidence and trust.'" (quoting *Trammel*, 445 U.S. at 51)).

191 *See Trammel*, 445 U.S. at 51 ("The priest-penitent privilege recognizes the human need to disclose to a spiritual counselor, in total and absolute confidence, what are believed to be flawed acts or thoughts and to receive priestly consolation and guidance in return.").

192 *See, e.g.*, Upjohn Co. v. United States, 449 U.S. 383, 392 (1981) (noting that the purpose of recognizing a privilege, such as the attorney-client privilege, is based in the desire that important, "relevant information" is shared between the parties).

193 *See Trammel*, 445 U.S. at 51 (discussing the multiple types of privileges and value each provides to the one sharing information in confidence).

194 *See supra* notes 188–91 and accompanying text.

Courts have widened the cadre of third-party confidants recognized by the attorney-client privilege even further to include members of the so-called "magic circle."[195] Common law courts recognized as long ago as the eighteenth century that there are certain third parties—like interpreters—who are crucial to the provision of legal advice.[196] If disclosure to these third parties breached confidentiality and resulted in privilege waiver, the attorney-client privilege itself would be compromised. Accordingly, courts hold that members of this magic circle do not count as third parties for privilege waiver purposes.[197] Today, members of the magic circle include language translators,[198] data analysts,[199] executive assistants,[200] IT support,[201] photocopy services,[202] necessary subject matter experts,[203] and the like. The magic circle is a circle of confidence.

Even divulging attorney-client communications to third parties outside of the magic circle and other privileged relationships will not necessarily result in waiver. The cornerstone of the privilege-waiver analysis is the intent of parties and the reasonableness of their precaution to preserve

---

195 United States v. Mass. Inst. of Tech., 129 F.3d 681, 687 (1st Cir. 1997) ("The privilege, it is said, is designed to protect confidentiality, so that any disclosure outside the magic circle is inconsistent with the privilege.").

196 Du Barré v. Livette (1791) 170 Eng. Rep. 96, 97; Peake 108, 110–11.

197 *See, e.g.*, Clay v. Williams, 16 Va. (2 Munf.) 105, 122 (1811) (acknowledging that a privilege based on confidentiality between an attorney and his client extends "even to interpreters going between the attorney and his client").

198 *See, e.g.*, Allied Irish Banks, p.l.c. v. Bank of Am., N.A., 240 F.R.D. 96, 103 (S.D.N.Y. 2007) (noting that communications with an attorney through an interpreter are protected by the attorney-client privilege as an exception to the principle that communications in the presence of a third party destroy confidentiality).

199 *See, e.g.*, Williams v. Sprint/United Mgmt. Co., 464 F. Supp. 2d 1100, 1114 (D. Kan. 2006) (holding that an adverse impact analysis by an analyst was protected by the attorney-client privilege because the analysis data was gathered at the direction of counsel and the communications were made for the purpose of obtaining legal advice).

200 *See, e.g.*, City & Cty. of S.F. v. Superior Court, 231 P.2d 26, 30 (Cal. 1951) (en banc) (noting that the attorney-client privilege extends to employees such as "the attorney's secretary, stenographer, or clerk regarding information of communications between attorney and client acquired in such capacities").

201 *See, e.g.*, Compulit v. Banctec, Inc., 177 F.R.D. 410, 412 (W.D. Mich. 1997) (holding "that a law firm does not waive its client's privilege by contracting with an independent contractor" who provides computer-assisted litigation support when it is done "to provide a necessary service that the law firm feels it needs in order to effectively represent its clients").

202 *See, e.g.*, *id.* ("[T]he attorney-client privilege [would not] be lost if a law firm used an outside document copy service or hired an independent document copy service to copy privileged communications.").

203 Symposium, *The Applicability of the Attorney-Client Privilege to Non-Testifying Experts: Reestablishing the Boundaries Between the Attorney-Client Privilege and the Work Product Protection*, 68 WASH. U. L.Q. 19, 22–23 (1990) (explaining the circumstances in which courts extend the attorney-client privilege to experts because those experts do not have a recognized privilege or the circumstances prevent the privilege from otherwise applying).

confidentiality.[204] Where the disclosure is inadvertent, "the relevant consideration is the intent of the defendants to maintain the confidentiality of the documents as manifested in the precautions they took."[205] Accordingly, courts ask whether the party claiming the privilege "took reasonable steps to prevent disclosure" and, upon discovering it, "promptly took reasonable steps to rectify the error."[206] A typical sort of case involves parties who inadvertently produce privileged documents in response to a discovery request.[207] Courts will inquire into the steps the party took before disclosure—e.g., conducting pre-production privilege review of the documents—and after—e.g., promptly requesting return of the documents upon learning of a mistake.[208]

Some waiver cases specifically address the knowing disclosure of attorney-client communications to third-parties who are not the direct recipients of the information, but merely aide its transmission. These cases are most analogous to the central concern of this Article—how third-party service providers affect privacy under the Fourth Amendment. In the privilege context, these third parties facilitate, have access to, store, or monitor communications that include attorney-client communications, such as cell-service providers, internet service providers, or employer-provided email systems.[209] Courts have adapted the centuries-old law of attorney-client privilege to modern contexts and technologies.[210] The underlying

---

204 *See* Rice, *supra* note 178, at 853–55 ("In all formal definitions of the attorney-client privilege, whether employed in state or federal courts, the client or the attorney must communicate with the other in confidence, and subsequently that confidentiality must have been maintained." (footnotes omitted)).

205 Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 260 (N.D. Ill. 1981).

206 FED. R. EVID. 502(b).

207 *See* Alldread v. City of Grenada, 988 F.2d 1425, 1433 (5th Cir. 1993) (noting that privileged tapes were inadvertently shared during discovery); Transamerica Comput. Co. v. Int'l Bus. Machs. Corp., 573 F.2d 646, 647 (9th Cir. 1978) (noting that the inadvertent disclosure in question occurred during accelerated discovery proceedings).

208 *See Suburban Sew 'N Sweep, Inc.*, 91 F.R.D. at 260–61.

209 *See, e.g.*, Edward J. Imwinkelried, *The Applicability of Privileges to Employees' Personal E-mails: The Errors Caused by the Confusion Between Privilege Confidentiality and Other Notions of Privacy*, 2014 MICH. ST. L. REV. 1, 3–4 (discussing the status of the law regarding the applicability of the attorney-client privilege to emails that are subject to employer monitoring); Anne Klinefelter, *When to Research Is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1, 29 (2011) (explaining how internet activity tracking conducted by websites, advertisers, and internet service providers may lead courts to find waiver of the privilege in some cases); Timothy Peterson, *Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege*, 46 J. MARSHALL L. REV. 383, 396 (2012) (discussing how the law has not yet established rules governing attorney-client privilege and confidentiality and new technologies such as cloud computing, leading to risks of privileged material being disclosed to non-privileged third parties).

210 *See* JEROME G. SNIDER & HOWARD A. ELLINS, CORPORATE PRIVILEGES AND CONFIDENTIAL INFORMATION § 2.08 (1999) ("[M]any important issues currently at the center of the privilege

doctrinal and normative framework of the attorney-client privilege has shown itself to be more adaptable than the much more recent privacy doctrines of the Fourth Amendment.

Once again, standards of reasonableness govern whether clients waive privilege by using third-party services to communicate with their attorneys. Accordingly, courts assess the matter on a case-by-case basis,[211] and the balance can tip in either direction.[212] In one common fact pattern, an employee in *Stengart v. Loving Care Agency, Inc*. used a work-issued device to send messages to her attorney over a private email account.[213] The device utilized a program that captured a picture of every website the employee visited, and the employer had a device policy in place that granted it access to any records on its computers.[214] The central concern for the court was whether the employee had a "reasonable expectation" of confidentiality in the emails despite the employer's software and policy.[215] The court balanced the employer's access against several specific facts, including that the employee used her personal email account, over a web-based platform, and without storing her password on the device.[216] These steps, in addition to

discussion concern new technology."); Mitchel L. Winick et al., *Playing* I Spy *with Client Confidences: Confidentiality, Privilege and Electronic Communications*, 31 TEX. TECH L. REV. 1225, 1227 (2000) ("[E]ach modern technological advance has taken attorneys and their clients one step farther from the closed-door, personal interactions upon which the privilege was founded. Accordingly, with each step, the legal profession has been confronted with challenges to the privilege." (footnote omitted) (citing Stephen M. Johnson, *The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet*, 50 ADMIN. L. REV. 277, 331 (1998))).

211 O'Connor v. Ortega, 480 U.S. 709, 710 (1987).

212 *See In re* Info. Mgmt. Servs., Inc. Derivative Litig., 81 A.3d 278, 287 (Del. Ch. 2013) ("Numerous courts have applied the *Asia Global* factors or closely similar variants when analyzing the attorney-client privilege [waiver claims premised on the use of unencrypted email]. Several of the *Asia Global* factors have been refined through subsequent application. In the current case, the *Asia Global* factors weigh in favor of production."); Imwinkelried, *supra* note 209, at 10 (discussing the factors that determine whether the attorney-client privilege applies); *see also* Kara R. Williams, *Protecting What You Thought Was Yours: Expanding Employee Privacy to Protect the Attorney-Client Privilege from Employer Computer Monitoring*, 69 OHIO ST. L.J. 347, 356–58 (2008) (outlining different jurisdictions' evaluation of attorney-client privilege and e-mails over employer-owned e-mail systems). *Compare* Nat'l Econ. Research Assocs. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, at *4 (Mass. Super. Ct. Aug. 3, 2006) (finding that the attorney-client privilege did attach to e-mails sent over company system), *with* Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, 443 (Sup. Ct. N.Y. Cty. 2007) (finding that the privilege did not attach to e-mails sent over the employer's system).

213 990 A.2d 650, 655 (N.J. 2010).

214 *Id.* at 655–57.

215 *Id.* at 660. The court uses the phrase "reasonable expectation of privacy." However, since the conception of privacy is different from the one at play in the Fourth Amendment context, it is clearer for present purposes to use "confidentiality," the term more commonly associated with the attorney-client privilege.

216 *Id.* at 663–65.

the fact that the employer's device policy was not clearly communicated to employees, were sufficient to establish her expectation of confidentiality and to preserve the privilege of her attorney communications.[217]

As a general rule, the use of an unencrypted, third-party email service does not, by itself, suffice to waive attorney-client privilege.[218] In *In re Asia Global Crossing*, a leading case on the matter, officers of a bankrupt corporation used the corporate e-mail system to communicate with their personal attorneys about their claims against their employer.[219] The corporate trustees argued that the officers had waived their privilege on several grounds: e-mail carries an inherent risk of disclosure, the e-mail system was owned and run by the corporation, and the system policy prohibited its use for confidential communications.[220] Following the stance of the American Bar Association and some state bar associations,[221] the court held that "lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality."[222] But, the court did acknowledge that some uses of employer email could result in waiver. It said that four main factors bear on the analysis:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[223]

The *Asia Global* court applied the factors and found "the use of the company's e-mail system d[id] not, without more, destroy the privilege."[224] Other courts have relied on the *Asia Global* factors to guide their waiver inquiry.[225]

The general rule is that clients can maintain their reasonable expectation of confidentiality, even when they know third-party facilitators may be

---

217 *Id.* at 664–65.

218 *In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005) ("[T]he transmission of a privileged communication through unencrypted e-mail does not, without more, destroy the privilege.").

219 *Id.*

220 *Id.* at 259–60.

221 Micah K. Story, *Twenty-First Century Pillow-Talk: Applicability of the Marital Communications Privilege to Electronic Mail*, 58 S.C. L. REV. 275, 295 (2006).

222 *Asia Glob. Crossing*, 322 B.R. at 256.

223 *Id.* at 257 (footnote omitted).

224 *Id.* at 251.

225 *See, e.g.*, Ala. Aircraft Indus., Inc. v. Boeing Co., No. 2:11-CV-03577-RDP, 2016 WL 7745029, at *5 (N.D. Ala. Dec. 2, 2016); *In re* High-Tech Emp. Antitrust Litig., No. 11-CV-2509-LHK-PSG, 2013 WL 772668, at *5–6 (N.D. Cal. Feb. 28, 2013); *In re* Reserve Fund Secs. & Derivative Litig., 275 F.R.D. 154, 159–60 (S.D.N.Y. 2011).

looking on, by taking "affirmative steps to maintain the confidentiality of the attorney-client communications."[226] If the client does not take these steps, waiver will result. In *Harleysville Insurance Co. v. Holding Funeral Home, Inc.*, the court held that posting case files and communications to an online storage system without sufficient precautions to prevent access by a third party constitutes a waiver of the attorney-client privilege.[227] Attorneys had posted the information to a file sharing site for use by Harleysville's attorneys.[228] In the course of explaining its decision, the court noted some easy precautions the attorneys could have taken to prevent waiver, such as password protecting the files[229] or safeguarding the access link.[230] As it was, the client had done "the cyber world equivalent of leaving [a] claims file on a bench in the public square and telling its counsel where they could find it."[231]

Interestingly, courts that have analyzed privilege waiver in the context of third-party electronic service providers—like email and cloud storage—focus on the possibility of waiver due to access by yet other third parties—like employers or opposing counsel. The third-party service providers usually seem to recede into the background, like people in other privileged relationships with the client or the "magic circle" that is necessary for facilitating attorney-client communication. This cannot be because courts are only concerned with whether opposing parties could access the communications. Unlike the work-product protection,[232] disclosure to any third party potentially waives attorney-client privilege if the disclosure calls the confidentiality of the communication into question.[233] Rather, it must be because courts do not regard the use of such service providers, which most

---

226 Geer v. Gilman Corp., No. 3:06 CV 889(JBA), 2007 WL 1423752, at *4 (D. Conn. Feb. 12, 2007).

227 Harleysville Ins. Co. v. Holding Funeral Home, Inc., No. 1:15cv00057, 2017 WL 1041600, at *9 (W.D. Va. Feb. 9), *overruled in part by* 2017 WL 4368617 (W.D. Va. Oct. 2, 2017).

228 *Id.* at *2.

229 *Id.*

230 *Id.*

231 *Id.* at *9. The magistrate judge's opinion in *Harleyesville* was eventually reversed by the reviewing district court judge. Harleysville Ins. Co. v. Holding Funeral Home Inc., 1:15CV00057, 2017 WL 4368617, at *19 (W.D. Va. Oct. 2, 2017) (finding reasonable precautions were taken in part because files uploaded to cloud server were accessible only using a randomly generated URL that was not discoverable using Google or other web search engines). The contrasting opinions on the case illustrate both how judges will sometimes find that precautions to preserve confidentiality against third-party service providers are insufficient, and also how low the bar to preserve confidentiality can be.

232 *See In re* Chevron Corp., 633 F.3d 153, 165 (3d Cir. 2011) (stating that disclosure to a third party waives the attorney-client privilege, but the work product privilege is only waived if disclosure is to an adversary). The work-product protection is a weaker privilege. *See* United States v. Nobles, 422 U.S. 225, 239 (1975) (stating that the work-product privilege is "not absolute"). It applies only to documents prepared by an attorney in anticipation of litigation. *Id.* at 238.

233 *Chevron Corp.*, 633 F.3d at 165.

attorneys and clients need to communicate at all, to be inherently inconsistent with the confidentiality of those communications.

In sum, the notion of privacy courts use in the context of the attorney-client privilege reflects an intuitive understanding of privacy as a form of confidentiality. "Confidence" has its roots in the Middle French and Latin words meaning "trust."[234] Confidence and trust have a different informational logic than the sort of secrecy which is the current lynchpin of Fourth Amendment jurisprudence. Like secrecy, confidentiality can be lost when third parties get involved. Sharing information with third parties can signal that it is not shared under conditions of mutual trust. But unlike secrets, confidential information does not necessarily become less confidential when shared. One can have a reasonable expectation of confidentiality with another person; but there is something paradoxical about insisting what you tell another is truly secret. To determine whether attorney-client communications remain confidential despite disclosure to third parties, courts ask whether the client had subjective and objective expectations of confidentiality. The latter is measured by whether the client took reasonable precautions to maintain the confidential nature of the communication.

III. REASONABLE EXPECTATIONS OF CONFIDENTIALITY

Privacy is at the heart of Fourth Amendment law. There are multiple, overlapping ways to understand what privacy is. Fourth Amendment jurisprudence and the common law of attorney-client privilege offer competing conceptions. Both recognize that sharing information can compromise its privacy. However, under the Fourth Amendment's understanding of privacy-as-secrecy, the fact that information has been shared is usually dispositive of its lost privacy. Privacy-as-confidentiality in the law of attorney-client-privilege is more nuanced—with appropriate precautions, information can remain confidential even if third parties have access to it.

The Supreme Court should abandon its understanding of privacy as a type of secrecy and import the common law understanding of privacy-as-confidentiality. This would allow the Court to strike a more appropriate balance between the interests of investigating authorities and the interests of the people in their personal data. Thinking of privacy-as-confidentiality under the Fourth Amendment would soften the force of the third-party doctrine where third-party service providers are involved. Under current

234 *See Confide*, THE CONCISE OXFORD DICTIONARY OF ENGLISH ETYMOLOGY (T.F. Hoad ed., 1996).

law, the Fourth Amendment does not protect what is quickly becoming the bulk of our intimate information because third-party service providers—like cell companies and ISPs—have access to it. Thinking of privacy as confidentiality could change this. The move should be easy for the Court to make since the attorney-client privilege is backed by centuries of judicial refinement and application to a wide range of cases. It should also not require a large shift in core Fourth Amendment jurisprudence outside of the third-party service provider context. Secret information is by its nature also confidential. So key Fourth Amendment rights would remain in place. These rights would just extend under this proposal in a more sensible way to a modern world held together by third parties.

Most of the Justices in *Carpenter*, in both the majority and dissent, were searching for conceptual tools to convey that "a third party [having] access or possession of your papers and effects does not necessarily eliminate your interest in them."[235] Doing this by shifting to a conception of privacy as confidentiality has several distinct advantages over the proposal they hit upon. The majority's solution—carving seven-day blocks of cell-site location information out for special treatment—is an ad hoc solution. As Justice Gorsuch asks, "[W]hat distinguishes historical data from real-time data, or seven days of a single person's data from a download of everyone's data over some indefinite period of time?"[236] Justice Kennedy felt similarly, referring to the "arbitrary 6-day cutoff."[237]

In addition to being ad hoc, the majority's approach does not go far enough to explain why "[j]ust because you entrust your data . . . to a third party may not mean you lose any Fourth Amendment interest in its contents."[238] Justice Gorsuch makes the intuitive point:

> Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to manifest my willingness to accept the risk that the government will pry the document from my friend and read it without his consent?[239]

The precedent established by the *Carpenter* majority does not protect Fourth Amendment interests in any other information people reveal to third party

---

235 Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting); *id.* at 2221 (majority opinion) ("[T]hird parties . . . [hold] records in which the suspect has a reasonable expectation of privacy.")

236 *Id.* at 2267 (Gorsuch, J., dissenting) (emphasis omitted).

237 *Id.* at 2234 (Kennedy, J., dissenting).

238 *Id.* at 2269 (Gorsuch, J., dissenting) (emphasis omitted).

239 *Id.* at 2263 (internal quotation marks and emphasis omitted).

service providers, like six-day blocks of location information, emails, genomes, photos, etc. Conceiving of privacy as confidentiality would.

To the extent the majority means for its opinion to reach beyond seven-day blocks of cell-site location information,[240] it provides very uncertain guidance. The Court says the distinctive properties of cell-site location information deserve Fourth Amendment protection, but fail to say clearly what those distinctive properties are.[241] Justice Kennedy predicts that the "newly conceived constitutional standard will cause confusion" among lower courts and enforcement personnel.[242] In his view, the Court has effectively set up an unprincipled "balancing test . . . . [that just asks when] privacy interests are weighty enough to 'overcome' the third-party disclosure."[243] Without more guidance on how, if at all, to extend the *Carpenter* precedent to different types of information, Justice Kennedy must be right. The solution proposed here is different. Since it draws on centuries of attorney-privilege precedent, it offers a more robust framework for assessing a broad range of information types and contexts.

The next two Sections describe in more detail what the Fourth Amendment inquiry into reasonable expectations of privacy-as-confidentiality would look like.

A. An Open-Textured Inquiry

On the approach proposed here, the Fourth Amendment's warrant requirement protects personal information when, and only when, a person has a reasonable expectation of confidentiality in it. As under current Fourth Amendment[244] and attorney-client privilege[245] case law, the confidentiality inquiry would have both subjective and objective components. What follows explores these components where third-party service providers are involved. Though not a focus of the discussion, the considerations raised below could extend to other sorts of third parties, including natural persons.

---

240 *Id.* at 2214 (majority opinion) ("[W]e reject[ ] . . . a mechanical interpretation of the Fourth Amendment." (internal quotation marks and emphasis omitted)).

241 *Id.* at 2232 (Kennedy, J., dissenting) ("[T]he Court maintains, cell-site records are 'unique' . . . . But many other kinds of business records [are similar]. . . .").

242 *Id.* at 2230.

243 *Id.* at 2231–32.

244 *See supra* notes 29–38 and accompanying text.

245 *See supra* notes 150–52 and accompanying text.

1. Subjective Expectation

Courts should first ask whether a person claiming Fourth Amendment protections had a subjective expectation that her information was and would be kept confidential. As under current Fourth Amendment law, this could mean that the person actually thought that the information was and would be kept secret.[246] But a subjective expectation of confidentiality could remain even where the person has voluntarily shared it with a third party and so knows the information is not secret. These sorts of cases could potentially fall into three categories, all of them recognized by privilege law.

First, the person may feel she is in a *relationship of trust* with the third party. Mutual trust is crucial to the analysis in attorney-client privilege contexts where third parties are involved.[247] People trust those with whom they are in confidential relationships not to disclose their information in ways that would disadvantage them. This does not necessarily mean that people expect their trusted third parties to keep their information secret. Sometimes, as with an attorney's magic circle, the third party must disclose the information to fourth and fifth parties for the ultimate benefit of the person whose information it is. This is an expected feature of confidential (as opposed to secretive) relationships. However, a subjective expectation of confidentiality could not exist where the information holder believes there is some likelihood the third party (e.g., an attorney or a service provider) may expose the information to her disadvantage (e.g., to her adversary or to government investigators without a warrant).

Courts have formally recognized that some sorts of relationships are presumptively confidential in this way, like the spousal relationship or the confessional relationship.[248] But subjective expectations of trust and confidentiality can extend beyond these. People may even feel that they have such relationships with corporate third-party service providers.[249] Indeed such companies often invest a lot into cultivating customer trust and

246 *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that monitoring a person's home with thermal imaging technology was a search under the Fourth Amendment because the defendant had a reasonably expectation of privacy, secrecy, in his conduct in his own home).

247 *See* Mark J. Kadish, *The Attorney-Client Privilege: Can It Stand Its Ground Against New Government Intrusions?*, 36 EMORY L.J. 793, 793 (1987) (describing mutual trust as one of the cornerstones of the attorney-client privilege).

248 *See supra* notes 159–63 and accompanying text.

249 *See* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (recognizing that in many circumstances, the fact that an internet service provider has control over and access to emails is alone insufficient to eliminate a person's expectation of privacy in those emails).

reputations for discretion.[250] Facebook offers "privacy" settings, which can make us feel that they respect the confidentiality of the personal information we protect using them.[251] Apple publicly resists federal government pressure to unlock the iPhones of criminal suspects[252] in an effort to give the impression that the company respects privacy.[253] Whether it is reasonable for customers to buy into these marketing campaigns is a separate question. That customers frequently do is clear from companies' continued investment.

Second, a person may have a subjective expectation of confidentiality while utilizing a third-party service provider because *she may not know that the third-party service provider has access to her information*. Third-party service providers design their products to minimize our awareness that at each moment they are collecting, storing, and processing our information.[254] They do this in part because they want clean information about our habits and preferences, and people who feel they are being observed modify their behavior.[255] The information from our web searches, product purchases, geolocation, etc., is less valuable to advertisers when it is not authentic.[256] So

---

250 *See* JONATHAN R. MACEY, THE DEATH OF CORPORATE REPUTATION: HOW INTEGRITY HAS BEEN DESTROYED ON WALL STREET 8 (2013) ("Firms invest in reputation so that customers will do business with them. Rational customers prefer to do business with companies with good reputations because a strong reputation for honesty and integrity serves as a sort of bond, or credible promise to customers that the business will not act in a dishonest or immoral way. . . . [A]ccording to the traditional economic theory of reputation, simple cost-benefit analysis predicts that companies will invest in reputation because doing so enables them to attract customers who will pay a premium to deal with the company with the good reputation.").

251 *See Basic Privacy Settings & Tools*, FACEBOOK, https://www.facebook.com/help/325807937506242 (last visited Dec. 2, 2018).

252 *See, e.g.*, Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.

253 *Id.* (reporting that Apple refused to create a "backdoor" to its iPhone's programming because of the threat it posed to all its customers' devices in the future).

254 *See, e.g.*, Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1434–35 ("[W]e adore Google for its simple, modest-looking interface masking a hyper-complicated algorithm. We admire it for providing superb services at no (evident) cost . . . . [But] [e]very day, millions of users provide Google with unfettered access to their interests, needs, desires, fears, pleasures, and intentions. Many users do not realize that this information is logged and maintained in a form which can facilitate their identification.").

255 *See, e.g.*, Melissa Bateson et al., *Cues of Being Watched Enhance Cooperation in a Real-World Setting*, 2 BIOLOGY LETTERS 412, 412 (2006) (reporting that people contributed nearly three times as much money to a coffee room honesty box when a picture of eyes was present on a nearby wall than when a picture without eyes was on the wall).

256 *See* Natasha Singer, *Your Online Attention, Bought in an Instant*, N.Y. TIMES (Nov. 17, 2012), http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-

third-party service providers try to make us feel that we truly are by ourselves when we are on our smartphones late at night.[257] As discussed above, there are in fact any number of trackers operating behind the scenes watching our digital trails.[258] As courts have repeatedly held in the attorney-client privilege context, a person who is not aware that others are accessing her information can have no reason to doubt its confidentiality.[259]

The third sort of case is subtler—where a person knows she is sharing information with a third-party service provider, even one she does not trust, but *believes it is practically certain that the information is not identifiable as* her *personal information*. This is a safety-in-numbers sort of rationale. In many circumstances, customers will have agreed to let third-party service providers access and use their information, even though they do not necessarily feel that they are in a relationship of trust with the company. By clicking "I Agree" before installing a smartphone app, downloading a new browser, or signing up for internet service, customers usually grant the service provider access to their information.[260] Sometimes people do not read or understand

---

by-advertisers.html (discussing how online advertising has moved away from traditional forms of "spray and pray" advertising to using complex algorithms that instantly analyze an internet user's search and website history and instantaneously sell advertising space targeted at the specific searcher).

257 *See generally Hidden Brain: What Our Google Searches Reveal About Who We Really Are*, NPR (May 1, 2017, 9:01 PM), https://www.npr.org/2017/05/01/526399881/what-our-google-searches-reveal-about-who-we-really-are.

258 *See supra* notes 55–66 and accompanying text.

259 *See* Sackman v. Liggett Grp., Inc., 173 F.R.D. 358, 365 (E.D.N.Y. 1997) (holding that attorney-client privilege was "not waived through public disclosure of a stolen privileged document"); *see also In re* Fattah, 802 F.3d 516, 530 (3d Cir. 2015) (holding that the government had to revise its search process of an email account in order to protect communications falling under the attorney-client privilege even though the emails were being provided directly from a third-party service provider); Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387, at *8 (E.D.N.Y. May 15, 2006) (holding that attorney-client privilege was not waived when an employer recovered emails from a company computer that was used at the employee's home because the employee had a reasonable expectation that personal communications on that computer were not monitored).

260 *See* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 15 (2005) ("Many [companies] voluntarily publish privacy policies, but there is no law requiring privacy policies or prescribing their content." (footnote omitted)). There are both federal and state laws that require a company to post a privacy policy in certain circumstances, but no general law requiring a policy in every circumstance. *See, e.g.*, 16 C.F.R. § 312.3(a) (2012) (requiring websites directed at children to "[p]rovide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information"); CAL. BUS. & PROF. CODE §§ 22575(a)–22578 (West 2014) (requiring operators of commercial websites or online services that collect personal information about individual consumers residing in California who use or visit its commercial website or online service to "conspicuously post its privacy policy on its Web site").

the policies they are agreeing to.[261] These scenarios would be examples of the second type of case.

Sometimes, though, people do read privacy policies, fully understand them, click "I Agree," and still retain a subjective expectation of confidentiality. The most obvious sorts of cases would be where the third-party service actually requires this information to function. People have to disclose their location to use mapping services like Google Maps. Though they share this sort of information with third-party service providers, they could believe that their information will be used consistently with its confidentiality. Third-party service providers often emphasize that the data they collect is anonymous, stripped of any personally identifying information.[262] People reading such policies often feel that their anonymous data will be just so many bits in a sea of bytes for millions of other accounts.[263] The customer may feel practically certain that neither the third-party service provider nor anyone else with access to her information would have the ability to collect her data and tie it specifically to her. Practical certainty is

---

261 Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 588 (2007) ("[M]ost studies show that, while consumers are increasingly concerned about the privacy of their personal information, they are still not likely to read—much less understand—online privacy policies." (footnote omitted)).

262 *See, e.g.*, *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 268–69 (3d Cir. 2016) (noting that the defendant company included a message that said, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" on the registration form for a website designed for children).

263 *See* Simon Hill, *How Much Do Online Advertisers Really Know About You? We Asked an Expert*, DIGITAL TRENDS (June 27, 2015, 3:00 AM), https://www.digitaltrends.com/computing/how-do-advertisers-track-you-online-we-found-out ("We know that companies are collecting data about us, but there's very little transparency in terms of the techniques they use, and there are a lot of misconceptions. [People] don't really know exactly what data [online trackers] are collecting, or what they might use it for."); *Special Report: Getting to Know You*, ECONOMIST (Sept. 11, 2014), https://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party ("As more information is attached to cookies and devices, it becomes easier to identify users, says Ed Felten, a professor of computer science at Princeton University. Mr[.] Felten and others have shown that, given enough information, anonymous data sets can be de-anonymised. One study found that it took only two data points to identify more than half the users. 'The idea of personally identifiable information not being identifiable is completely laughable in computer-science circles,' says Jonathan Mayer, a Stanford University computer-science researcher."); Manoush Zomorodi, *Do You Know How Much Private Information You Give Away Every Day?*, TIME (Mar. 29, 2017), http://time.com/4673602/terms-service-privacy-security (describing the "privacy paradox," in which most people say they care deeply about the privacy of their information yet continue to freely give it and allow it to be tracked online because they see no clear future consequences of giving up the information or figure that algorithms cannot do as much as they actually can); *see also* Tene, *supra* note 254, at 1435 ("Every day, millions of users provide Google with unfettered access to their interests, needs, desires, fears, pleasures, and intentions. Many users do not realize that this information is logged and maintained in a form which can facilitate their identification.").

not full certainty, but it may be enough for maintaining a subjective expectation of confidentiality.

If someone shredded an attorney-client communication and cast the pieces to the wind, courts would find this consistent with maintaining a subjective expectation of confidentiality, despite the remote possibility that another person may collect the bits and reconstruct the communique.[264] Courts have held that a subjective expectation of confidentiality can survive much lower levels of certainty. For example, an employee sending email over a company device may have a subjective expectation of confidentiality despite explicit company policy to the contrary if the company's practices "'lull[ed]' employees into believing that the policy would not be enforced."[265] Where the third party is an email provider rather than an employer, courts are even more likely to find the messages could have been sent with a subjective expectation of confidentiality,[266] despite the risk of exposure.

2. Objective Reasonableness

The three sorts of cases just considered only bear on whether a person can have a subjective expectation of confidentiality when interacting with a third-party service provider. Assuming the court finds she does, it should next ask whether that expectation was objectively reasonable. The Supreme Court currently takes a more or less categorical approach to assessing whether expectations of privacy are reasonable. The third-party doctrine categorically excludes any reasonable expectation of privacy in information shared with third parties. In the absence of a third-party issue, the Court recognizes categories of information over which people's expectations of privacy are presumptively reasonable, such as information contained in

---

264 *See* McCafferty's, Inc. v. Bank of Glen Burnie, 179 F.R.D. 163, 168 (D. Md. 1998) (suggesting that shredding privileged documents, as opposed to solely discarding them, would maintain the documents' confidentiality).

265 Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387, at *3 (E.D.N.Y. May 15, 2006).

266 *See* Sims v. Lakeside Sch., No. C06-1412RSM, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007) (contrasting employer monitoring with email client monitoring); *see also* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (finding a reasonable expectation of privacy in emails sent through AOL because AOL had strict privacy guidelines under which it would only disclose a client's emails to a third party if required by court order).

private residences,[267] hotel rooms,[268] many areas of commercial premises,[269] and private areas in public places such as restrooms and fitting rooms.[270]

Assessing the reasonableness of an expectation of privacy-as-confidentiality calls for a more fact-intensive, open-textured inquiry. This is usually how reasonableness judgments are supposed to work.[271] It is the sort of inquiry that courts making privilege-waiver determinations use.[272] The basic issue is not whether the information fits into some predetermined category or whether it has been shared. Rather, the underlying issue is whether the person claiming the privilege took reasonable steps, in light of the nature of the information and the circumstances, to preserve confidentiality. This requires courts to engage in a subtle balancing of the facts in any particular case to reach an all-things-considered judgment.

When third-party service providers are involved, courts assessing Fourth Amendment protections would first have to determine what level of attention to preserving confidentiality the circumstances called for. Some features of the circumstance would call for higher levels of care and others may call for lower. It would be impossible to list all possible considerations ex ante, but attorney-client privilege case law provides some representative factors. Courts have held that the following circumstances suggest that more care is needed to preserve confidentiality where third-party service providers are concerned:

---

267 Silverman v. United States, 365 U.S. 505, 511 (1961) ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

268 Stoner v. California, 376 U.S. 483, 490 (1964) ("[A] guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures.").

269 See v. City of Seattle, 387 U.S. 541, 543 (1967) ("The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property. The businessman, too, has that right placed in jeopardy if the decision to enter and inspect for violation of regulatory laws can be made and enforced by the inspector in the field without official authority evidenced by warrant.").

270 *See, e.g.*, State v. Bryant, 177 N.W.2d 800, 803 (Minn. 1970) (finding a reasonable expectation of privacy in a public restroom because, referencing *Katz v. United States*, 389 U.S. 347 (1967), "the facilities provided assure the user of privacy as much as a telephone booth does").

271 *See* Bonivert v. City of Clarkston, 883 F.3d 865, 872 (9th Cir. 2018) (stating that the test for reasonableness under the Fourth Amendment "is inevitably a fact-intensive inquiry"); Jason M. Solomon, *Juries, Social Norms, and Civil Justice*, 65 ALA. L. REV. 1125, 1128 (2014) (explaining how questions in law often come to questions of reasonableness and that questions of reasonableness are fact-intensive).

272 *See, e.g.*, Gray v. Bicknell, 86 F.3d 1472, 1484 (8th Cir. 1996) (adopting in a case regarding inadvertent disclosure of privileged communications a test that looks to the reasonableness of the precautions undertaken by the privilege holder to prevent a loss of confidentiality in the privileged documents).

- Electronic service monitoring policies, especially for employer-provided services;[273]
- Using devices provided by third parties, especially through employers;[274]
- Ability of a device on its own to inadvertently disclose communications;[275]
- Whether communications travel through public as opposed to private routes;[276]
- The number and types of individuals who have access to information that is stored with a third-party service provider;[277] and
- Whether the third-party service is a sharing service.[278]

---

273 *See In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (adopting a four-part test that focuses primarily on questions regarding the extent to which the party providing an internet-based service has adopted policies regarding the privacy of those who use its service).

274 *See, e.g.*, Sims v. Lakeside Sch., No. C06-1412RSM, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007) (finding no reasonable expectation of privacy when a plaintiff used an employer-provided email account on an employer-provided laptop).

275 *See, e.g.*, Huff v. Spaw, 794 F.3d 543, 552 (6th Cir. 2015) (holding that a reasonable expectation of privacy in communications over a cell phone was lost when the confidential information was conveyed inadvertently through a "pocket-dial"). "In sum, a person who knowingly operates a device that is capable of inadvertently exposing his conversations to third-party listeners and fails to take simple precautions to prevent such exposure does not have a reasonable expectation of privacy with respect to statements that are exposed to an outsider by the inadvertent operation of that device." *Id.*

276 *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (noting that emails sent through AOL carried a higher expectation of privacy than messages sent in other ways over the internet because the AOL emails were transferred through and stored on AOL's servers and databases as opposed to passing through normal internet servers).

277 *See, e.g.*, Willis v. Willis, 914 N.Y.S.2d 243, 245 (N.Y. App. Div. 2010) (holding that although emails with an attorney were sent over a private email account, the fact that the plaintiff's children knew the password to her account and frequently used the account for their own purposes removed her expectation of privacy). *But see* Geer v. Gilman Corp., No. 3:06 CV 889(JBA), 2007 WL 1423752, at *4 (D. Conn. Feb. 12, 2007) (noting that although the plaintiff used her fiancé's computer and email account to communicate with her attorney, the relationship between them was sufficiently close and analogous to an agency relationship that confidentiality was not waived).

278 *See, e.g.*, United States v. Pirosko, 787 F.3d 358, 371–72 (6th Cir. 2015) (finding no reasonable expectation of privacy to a file that was shared); *see also* Harleysville Ins. Co. v. Holding Funeral Home, Inc., No. 1:15CV00057, 2017 WL 4368617, at *7 (W.D. Va. Oct. 2, 2017) (finding that reasonable precautions had been undertaken, despite the fact that the information was stored on a cloud sharing service and had been inadvertently disclosed).

These factors should be balanced against others that have been held to lower the level of required care:

- Non-enforcement or unclear presentation of monitoring policies;[279]
- Presence of user-controlled privacy settings;[280]
- Ability to set passwords on private services;[281] and
- Contractual obligations of privacy between customer and third-party service provider.[282]

After the court has considered the circumstantial factors bearing on the level of care needed to preserve a reasonable expectation of confidentiality, it would assess whether the person with an interest in the information took appropriate steps. Once again, attorney-client privilege case law suggests representative steps that a person could take in the presence of third-party service providers to preserve the confidentiality of their information:

- Using and not disclosing passwords;[283]
- Adjusting privacy settings;[284]
- Using private services as opposed to those provided by another party, such as an employer;[285]

---

279 *See* Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387, at *3 (E.D.N.Y. May 15, 2006) (evaluating whether an existing monitoring policy was being truly enforced in determining whether confidentiality existed); *In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 259 (Bankr. S.D.N.Y. 2005) (noting that the company neither announced nor effectuated a policy of email monitoring or announcing that emails over a company email belonged to the company); Nat'l Econ. Research Assocs., Inc. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, at *5 (Mass. Super. Ct. Aug. 3, 2006) (affirming that attorney-client privilege existed despite an employer policy regarding monitoring because the policy did not expressly state that messages sent over the internet through personal email accounts on an employer-provided computer would be saved and monitored).

280 *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010) (discussing the role that privacy settings play in determining an expectation of privacy).

281 *See* United States v. Nunez, No. 12 Cr. 778-2, 2013 WL 4407069, at *2 (S.D.N.Y. Aug. 16, 2013) (holding that attorney-client privilege was not waived in emails sent through Gmail account because the account was private and protected by a password that was not disclosed to third parties).

282 *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (noting that AOL's contractual obligation of privacy with its clients created a reasonable expectation of privacy).

283 *See, e.g.*, United States v. Ziegler, 474 F.3d 1184, 1190 (9th Cir. 2007) (finding that an employee had a reasonable expectation of privacy because he locked his offices and secured his computer with a password).

284 *See Crispin*, 717 F. Supp. 2d at 991 (remanding the question of an expectation of privacy in Facebook wall posts to the lower court with instructions to look to the plaintiff's privacy settings because "it appear[ed] . . . that a review of plaintiff's privacy settings would definitively settle the question").

285 *See, e.g.*, Sims v. Lakeside Sch., No. C06-1412RSM, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007) (finding a reasonable expectation of privacy in emails sent on an employer-provided laptop through personal email account, but not for confidential emails through an employer-provided email account).

- Deleting cookies and other online tracking mechanisms;[286] and
- Using encryption.[287]

These steps should be considered along with things a person may have done that would undermine the reasonableness of her expectation of confidentiality, such as:

- Storing the password in a place accessible to others;[288]
- Sharing passwords or accounts with others;[289] and
- Failing to delete information present on devices owned by a third party.[290]

The significance of any particular factor or step would be hard to predict in the abstract. Where the circumstances indicate a high threat to confidentiality—e.g., an email provider with a transparent policy of sharing user data—and the steps taken to preserve privacy are weak—e.g., failing to protect a user account with a password—the outcome under the privacy-as-confidentiality approach would likely be the same as under current Fourth Amendment law. However, where the threat to confidentiality is weak—e.g., an email provider with a protective privacy policy—and the steps taken are robust—e.g., using encryption services—thinking of privacy-as-confidentiality could lead to a different result. It would allow courts to recognize that in these cases, people still have the sorts of privacy interests the Fourth Amendment should be protecting despite the presence of a third-party service provider.

Between those two poles is a wide grey space that calls for judgment in light of specific facts. The next Section illustrates what that inquiry might look like.

---

286 *See* Anne Klinefelter, *When to Research Is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1, 29 (2011) ("[A]n attorney might be protected against a finding of waiver if she took reasonable precautions to avoid online research tracking, such as adjusting the settings on her internet browser software to prevent third-party cookies, using encryption to avoid deep packet inspection where possible, and adding software to the browser to prevent tracking by web bugs." (footnote omitted)).

287 *See id.*

288 *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 565 (S.D.N.Y. 2008) (warning that leaving a password stored on another's computer may be a factor that can lead to losing confidentiality because it gives another access to private communications).

289 *See, e.g.*, Willis v. Willis, 914 N.Y.S.2d 243, 245 (N.Y. App. Div. 2010) (finding no expectation of privacy where a password for a personal email account was shared with children who regularly used the same account).

290 *See Pure Power Boot Camp*, 587 F. Supp. 2d at 565.

B. Test Case: Carpenter v. United States

Change may be in the air. The Supreme Court has signaled in *Carpenter* its interest in paring back the current scope of the third-party doctrine.[291] The case was on appeal from the Sixth Circuit and asked whether people have protected Fourth Amendment interests in location data collected by cell service providers.[292] The Supreme Court made a surgical exception for such location data when the government seeks more than seven days' worth.[293] This Article has argued that the decision did not go far enough. Conceiving of privacy as confidentiality offers a path for reaching the same intuitively appealing result in *Carpenter* while providing a theoretically justifiable template for future applications.

Petitioner Timothy Carpenter was convicted for leading a team of fifteen other men in several armed robberies.[294] Carpenter's role was to plan the robberies and drive the getaway car.[295] Crucial to the government's case against him was cell-site data the FBI had obtained from MetroPCS and T-Mobile, Carpenter's wireless carriers.[296] When turned on, cell phones continuously search for and ping the nearest cell towers to route any calls.[297] Wireless carriers record the time and location of the cell towers to which individual phones connect.[298] The FBI obtained the cell-site data using the Stored Communications Act, which authorizes courts to grant orders for telecommunications records.[299] The Act requires investigators to provide "reasonable grounds to believe that . . . [the data sought] are relevant and material to an ongoing investigation."[300] With Carpenter's cell-site data in hand cataloguing nearly 13,000 location points,[301] the FBI could place him within a half-mile to two-mile distance of each of the robberies when they

---

291 *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018) (holding that police must obtain a warrant to access cell-site location records).

292 United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment."), *rev'd*, 138 S. Ct. 2206 (2018).

293 *Carpenter*, 138 S. Ct. at 2217 n.3.

294 *Id.* at 2212.

295 *Carpenter*, 819 F.3d at 884–85.

296 *Id*. at 885.

297 *Carpenter*, 138 S. Ct. at 2211–12; *see also* Kristi Winner, *From Historical Cell-Site Location Information to IMSI-Catchers: Why TriggerFish Devices Do Not Trigger Fourth Amendment Protection*, 68 CASE W. RES. L. REV. 243, 246–47 (2017) (arguing that cell-site location information does not protect a user's reasonable expectation of privacy).

298 *Carpenter*, 138 S. Ct. at 2211–12; Winner, *supra* note 297, at 244.

299 18 U.S.C. § 2703(d) (2012).

300 *Id*.

301 *Carpenter*, 138 S. Ct. at 2212.

occurred.[302]

Carpenter challenged the government's use of the cell-site data under the Fourth Amendment. If Fourth Amendment protections applied, the FBI would have needed a warrant before getting the information. This would have required a showing of "probable cause,"[303] considerably more than the "reasonable grounds" standard in the Stored Communications Act.[304] The trial court and the Sixth Circuit rejected Carpenter's arguments. The Sixth Circuit focused on the fact that the cell-site data contained only "routing information" necessary to "facilitate [Carpenter's] personal communications," not the "content of those communications themselves."[305] The court's underlying rationale was the third-party doctrine. Like envelope information that the post office needs to deliver a letter[306] or the phone number a telephone company needs to connect a call,[307] wireless providers need location information to provide their service.

The Sixth Circuit relied heavily on a foundational third-party doctrine case, *Smith v. Maryland*.[308] *Smith* held that, since the petitioner "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," he could have no expectation of its privacy.[309] The Sixth Circuit reasoned analogously that Carpenter voluntarily exposed his location information to third-party wireless carriers. Consequently, under the present understanding of privacy as a kind of secrecy, Carpenter could have no reasonable expectation of the information's privacy.[310]

The Sixth Circuit's conclusion in *Carpenter* feels incongruous with the Fourth Amendment's underlying concern for privacy. Carpenter's location may not have been secret—his wireless providers knew it. Yet it could reveal many things about him that are intuitively private—the therapist he sees, the

---

302 United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

303 *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . .").

304 *See Carpenter*, 138 S. Ct. at 2221 ("That showing [required under the Stored Communications Act] falls well short of the probable cause required for a warrant."); Erik E. Hawkins, *No Warrants Shall Issue but upon Probable Cause: The Impact of the Stored Communications Act on Privacy Expectations*, 4 WAKE FOREST J.L. & POL'Y 257, 257 (2014) (stating that the Stored Communications Act allows the government to obtain personal information at "a lower standard than probable cause").

305 *Carpenter*, 819 F.3d at 887.

306 *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

307 Smith v. Maryland, 442 U.S. 735, 743 (1979).

308 *See id.*; *Carpenter*, 819 F.3d at 888.

309 *Smith*, 442 U.S. at 744.

310 *Carpenter*, 819 F.3d at 888 ("[F]or the same reasons that Smith had no expectation of privacy in the numerical information at issue there, the defendants have no such expectation in the locational information here.").

lovers he has, the faith he professes, the entertainment he prefers, etc.[311] Judge Stranch saw this, but her hands were tied by the third-party doctrine and the Supreme Court's understanding of privacy-as-secrecy.

As we know, the Supreme Court reversed the Sixth Circuit decision by making an arbitrary exception to the third-party doctrine for seven-day blocks of cell-site data. It might have reached the same result—the officers investigating Carpenter needed a warrant—in a more principled way were Fourth Amendment privacy construed as confidentiality. The questions for the Court would have been whether, despite sharing his location information with his wireless carriers, Carpenter nonetheless maintained a subjective and reasonable expectation that the information was confidential. There can be no question of this for secrecy—a shared secret is no longer secret. For confidentiality, though, the matter is not so categorical. A court would have to consider in detail factual circumstances that might undermine an expectation of confidentiality and responsive conduct that may have maintained it.

The first issue is whether Carpenter had a subjective expectation of confidentiality. The fact that his phone shared his cell-site data with his wireless carriers certainly cuts against Carpenter, but not decisively. Recall that there are three sorts of cases where a person may maintain a subjective expectation of confidentiality despite sharing information with a third party—she is in a relationship of trust with the third party, she does not know she is sharing the information, or she believes that the information will be used in a way that respects its confidentiality. Since the case record is insufficient to assess fully whether Carpenter fell in any of these categories, what follows is some informed guesswork.

From the available record, there would not seem to be any basis for Carpenter to claim that he was in a relationship of trust with his wireless carriers. Absent some specific trust-inducing language in the carriers' privacy policy, that would be a tough argument to make since trust does not generally seem to be an aspect of relationships with wireless carriers. The specifics of the marketing materials Carpenter saw and of his interactions with in-store sales agents may affect the mix of facts in his favor. These may

311 Margaret E. Twomey, Note, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401, 411 (2015) ("Patterns and more personal information can be identified from the combination of such extensive information revealing such personal details as frequently visited houses of religion, multiple trips to the headquarters of a political party, or regular visits to a lover's house—information the court held should be protected by a warrant." (footnote omitted) (citing United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)).

have projected the impression that the companies were to be trusted. We do not have access to the nature of the marketing strategies MetroPCS and T-Mobile used toward Carpenter, but third-party service providers frequently claim to respect customer privacy.[312]

The more straightforward claim for Carpenter could be that he simply did not know that he was sharing his location information.[313] The wireless contracts Carpenter signed with MetroPCS and T-Mobile no doubt referenced their use of location information, but Carpenter may not have read them. Indeed, if he had read the contracts, he would have been in the distinct minority of wireless subscribers.[314] As it stands, there was not even any evidence that Carpenter was literate—in Detroit, where Carpenter's exploits took place, half of adults are functionally illiterate.[315]

The Sixth Circuit's argument was that "any cellphone user who has seen her phone's signal strength fluctuate must know that . . . her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."[316] There are several gaps in that short chain of reasoning.

- "*Any user who has seen her phone's signal fluctuate . . .*" There was no evidence that Carpenter did see his cell signal strength fluctuate. He operated in Detroit, where coverage maps for MetroPCS

312 *Our Privacy Commitments*, AT&T, http://about.att.com/sites/privacy_policy (last visited Mar. 8, 2018) ("We will protect your privacy and keep your personal information safe."); *Privacy Policy Summary*, VERIZON, http://www.verizon.com/about/privacy/privacy-policy-summary (last visited Mar. 8, 2018) ("At Verizon, we are committed to maintaining strong and meaningful privacy protections for customers.").

313 A similar argument could be made under current Fourth Amendment law. The third-party doctrine applies only where a person "voluntarily" shares information with third parties. John B. Wefing & John G. Miles, Jr., *Consent Searches and the Fourth Amendment: Voluntariness and Third Party Problems*, 5 SETON HALL L. REV. 211, 211 (1974) (discussing the voluntariness requirement of the third-party doctrine). A person who does not know she is sharing, does not do so voluntarily. *See* C.L. Ten, *Paternalism and Levels of Knowledge: A Comment on Rainbolt*, 3 BIOETHICS 135, 135–36 (1989) (discussing how insufficient knowledge precludes voluntary decisions and actions). But, as shown in the paragraphs that follow, courts applying the simplistic understanding of privacy-as-secrecy seem unprepared to engage in the careful factual analysis that voluntariness actually requires. Thinking in terms of privacy-as-confidentiality could put courts in the mindset to give the question the level of attention it requires.

314 *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 7:30 AM), http://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 (discussing research that ninety-one percent of people agree to terms of service without actually reading them).

315 *Nearly Half of Detroit's Adults are Functionally Illiterate, Report Finds*, HUFFINGTON POST (May 7, 2011, 12:58 PM), https://www.huffingtonpost.com/2011/05/07/detroit-illiteracy-nearly-half-education_n_858307.html.

316 United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

and T-Mobile show solid blocks of strong service.[317] Even if his signal did fluctuate between full strength and something slightly less, there was no evidence Carpenter would have noticed that—the service strength symbol is small and he would likely not have experienced much difference in service quality.

- "*Must know that . . . her phone 'exposes' its location to the nearest cell tower*." Even if Carpenter did notice his signal strength fluctuating at points, he may not have known that this was because cell towers were tracking his relative proximity. It takes some understanding of how the cell service works to appreciate this fact. While this may be obvious to the FBI agents who testified at Carpenter's trial,[318] most people (including the Author just a few years ago) use their cellphones unreflectively, trusting to the mysterious magic of technology.[319] For all the signal strength icons reveal, it could be based on how well the phone *receives* a signal, not how well it is transmitting a signal; the former would not convey anything about location back to the towers. What is more, there are many factors that can influence cell-signal strength even while a phone remains stationary, including weather conditions,[320] bits of aluminum foil,[321] or just

317 *Coverage Map*, METROPCS, https://www.metropcs.com/coverage.html (last visited Mar. 8, 2018); *Coverage Map*, T-MOBILE, https://www.t-mobile.com/coverage/coverage-map (last visited Mar. 8, 2018).

318 *See Carpenter*, 819 F.3d at 885 (discussing the trial testimony of an FBI agent who was familiar with cell network technology and described wireless carriers' coverage).

319 *See* Matt Bishop, *Technology, Training, and Transformation*, 8 IEEE SECURITY & PRIVACY 72, 72–73 (2010) (discussing how most consumers have little technical understanding of cellphones and other modern technology).

320 *Understanding Wireless Cellphone Coverage*, FCC (Oct. 27, 2017), https://www.fcc.gov/consumers/guides/understanding-wireless-telephone-coverage-areas ("[W]ireless phone calls can be affected by severe weather . . . . "); Duncan Graham Rowe, *Mobile-Phone Signals Reveal Rainfall: Wobbles in Transmissions Help to Create Weather Data*, NATURE (May 4, 2006), https://www.nature.com/news/2006/060501/full/news060501-10.html ("[R]ain can affect mobile-phone transmissions . . . .").

321 Bill Robertson, *Science 101: Q: Why Do You Lose AM Radio Reception When You Go Under an Overpass?*, 49 SCI. & CHILD. 67, 68 (2011) ("Just for kicks, wrap your cell phone in aluminum foil and try to call it. Nada, because cell phone signals are transmitted via electromagnetic waves."). This fact has led to the rise of a niche market for "Faraday bags" for knowledgeable, privacy sensitive individuals who want to prevent wireless carrier snooping. *See, e.g.*, FARADAY BAG, http://faradaybag.com (last visited Mar. 8, 2018).

touching the wrong spot on a phone's casing.[322] None of these has to do with a user's location.

- "*And thus [exposes her location] to the company that operates the tower*." Supposing Carpenter knew that his phone connects to the nearest cell towers, he still may not have known that the tower communicated this information in any way to his wireless carriers. People interact with third-party products all the time even though those products convey nothing about customers to the companies that own them. When someone passes through a third-party automatic barrier gate, the gate will not in most instances communicate who passed through the gate or when. If mounted with license plate scanners and connected to a network, it might, but most gates function fine without this hardware. The court record did not indicate whether the cell towers need to communicate with MetroPCS and T-Mobile to function, or whether knowledge of this necessity is widespread. There are certainly some third-party service providers who claim not to access, or even to be able to access, the information that their customers convey using the company hardware and software.[323] The Sixth Circuit suggested that Carpenter did not turn over the contents of his communications to his wireless carriers, even though these would have passed through the cell towers too.[324] Why should Carpenter be presumed to know that his cell-site location data was any different?

So, again depending on the specific facts, there would have been room for Carpenter to argue that he had a subjective expectation of confidentiality over his cell-site data because he trusted his wireless carriers and/or did not know his phone was sending this information to them. Carpenter could separately have argued that he expected them to use the information in ways consistent with the data's confidentiality. The record does not contain the actual service agreement that Carpenter signed with MetroPCS or T-Mobile. Reviewing the present privacy policies of these companies at the time of writing this Article is telling. They are far from transparent. T-Mobile gives the initial impression that the companies make temporary use of location data, and only for internal purposes. The agreement specifically

322 *See* Miguel Helft, *On New iPhone, a Mystery of Dropped Calls*, N.Y. TIMES (June 24, 2010), http://www.nytimes.com/2010/06/25/technology/25apple.html.

323 *Your Benefits with Boxcryptor*, BOXCRYPTOR, https://www.boxcryptor.com/en/ (last visited Nov. 2, 2018) (offering "[z]ero knowledge encryption").

324 United States v. Carpenter, 819 F.3d 880, 885–90 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

mentions location data: "We may use information about your location to provide our services or to customize data presented to you."[325] A straightforward reading of this phrase would suggest that these are the only uses to which that information would be put.[326] It is only by clicking on a further link, and reading through blocks of longer text in much smaller font that one finds that T-Mobile "may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement when . . . served with lawful process."[327] As Justice Gorsuch noted, "Consenting to give a third party access to private papers . . . is not the same things as consenting to a *search of those papers by the government*."[328] Carpenter, had he casually read the privacy policy, could reasonably claim surprise that T-Mobile shared his location information with further parties in the absence of a warrant.

Similarly, he could claim surprise that T-Mobile stored and recorded his location data. Using data for a limited and temporary purpose is more consistent with expectations of confidentiality than storing the information for later use. T-Mobile's privacy policy provides that the company "retain[s] information collected about [customers] for only as long as [the company] *need[s]* such information for business, legal, or tax purposes."[329] While T-Mobile could claim to "need" Carpenter's location data to route his calls, it is far from clear, and the record does not disclose, any further business, legal, or tax necessity for long-term records of the data. There may have been some business advantage to retaining the information, but "need" conveys something stronger and more limited.

If Carpenter could have established that he had a subjective expectation of confidentiality, he would then have had to persuade the court that his expectation was reasonable. The Sixth Circuit, thinking of privacy-as-secrecy, seemed of the categorical opinion that Carpenter's "conduct was not *and could not* have been calculated to preserve the privacy" of his location.[330] The analysis in terms of confidentiality would be much more nuanced. As in the privilege context, the court would have to balance factual

---

325 *T-Mobile Privacy Statement Highlights*, T-MOBILE (Dec. 31, 2016), https://www.t-mobile.com/company/website/privacypolicy.aspx (last visited Feb. 28, 2018) [https://perma.cc/8KQQ-F9YY].

326 ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 107 (2012) (explaining the canon of *expressio unius est exclusio alterius*, which stands for the idea that an affirmative statement makes a negative implication of its contrapositive).

327 *T-Mobile Privacy Statement Highlights*, *supra* note 325.

328 Carpenter v. United States, 138 S. Ct. 2206, 2263 (2018) (Gorsuch, J., dissenting).

329 *T-Mobile Privacy Statement Highlights*, *supra* note 325 (emphasis added).

330 United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) (emphasis added) (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979)), *rev'd*, 138 S. Ct. 2206 (2018).

circumstances that potentially undermine confidentiality with steps Carpenter took to preserve it. The main fact that Carpenter would have had to overcome to establish the reasonableness of his expectation is his formal agreement to his wireless carriers' privacy policies. These no doubt reflected that the companies would collect, could share, and might store his location information. In the absence of taking any steps to preserve confidentiality, this may be enough to defeat the reasonableness of Carpenter's expectation. Importantly, though, there are steps Carpenter could have taken to preserve his reasonable expectation of confidentiality.

The record does not reflect any precautionary steps Carpenter took. Under present understandings of the third-party doctrine, this is unsurprising—such details would not have been relevant anyway. The case law on privilege suggests several steps that could have been relevant:

- Turning off his phone except when needed. This would have prevented his phone from "pinging" nearby towers when it was not in use.
- Using a Faraday bag. This would have had the same effect as turning off his phone by cutting any communication between the phone and cell towers.
- Turning off his GPS. Cell-site location data is much less accurate than GPS.[331]
- Leaving his phone at home when possible.
- Password protecting his phone. This would have secured any location data stored on his phone from third parties who might try to access it.
- Using multiple phones and wireless carriers. This would have prevented any single source from having a consistent record of his location data.
- Using a location spoofer. These are apps that can scramble a phone's GPS location.[332]
- Updating phone and app settings so they did not store location records.

Of course, none of these steps, alone or in combination, could have *guaranteed* that Carpenter's location data would have remained confidential. That is not the question.[333] Rather, the courts should be asking whether,

---

331 *See id.* at 889 (discussing that, while GPS devices can be accurate within fifty feet, cell-site location merely identifies a wedge that ranges between one-half mile and two miles across that a cellphone is in).

332 *See* Nathan J. Buchok, *Plotting a Course for GPS Evidence*, 28 QUINNIPIAC L. REV. 1019, 1031 (2010) (discussing how a "spoofer" is able to deceive a GPS device about the spoofer's location).

333 *See Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting) ("[K]nowing about a risk doesn't mean you assume responsibility for it.").

given the necessity of cell phones to modern life, the way cell phones work, and the details of the privacy policy Carpenter signed, any steps he did take were reasonably calculated to justify an expectation of confidentiality. Just as courts assessing privilege find that there are steps employees can take to justify reasonable expectations of confidentiality in emails they send from employer monitored devices, there will be some steps that in combination could suffice in Carpenter's circumstances.

CONCLUSION

This Article proposes replacing the Supreme Court's current understanding of Fourth Amendment privacy. The concept usually goes undefined in the case law. The Court's development of the third-party doctrine—that privacy is generally lost when information is shared with third parties—reveals that its implicit understanding of privacy is as a type of secrecy. Thinking of privacy as secrecy is too restrictive in the modern world, where we must rely on third parties for our ordinary social and economic lives. A different area of privacy law—attorney-client privilege—is more adaptable and has already responded to the current state of technology. In privilege law, the relevant notion is privacy as a sort of confidentiality. Unlike secrets, confidential information can be shared with third parties, and still remain confidential with the right precautions.

If the Court drew on the developed common law of privacy-as-confidentiality, it would have the tools to respect the Fourth Amendment interests people have in personal communications that require the assistance of third-party service providers. When determining whether a person has a reasonable expectation of confidentiality in information shared with third-party service providers, a court's central questions would be:

1. Did the person have a subjective expectation that the third-party service provider would keep the information confidential?
2. Was that expectation reasonable? That is to say, in light of the circumstances, did the person take appropriate steps to preserve the confidentiality of the information?

Both of these questions call for case-specific inquiries, balancing features of the circumstance that may have called for caution, and the cautious steps taken in response. Courts assessing claims of attorney-client privilege have been answering these questions for cell phones, text messages, emails, and the like for decades. Their collective wisdom would be a powerful resource for courts assessing confidentiality in the context of the Fourth Amendment in the modern age.

As with any standard, the fact-specific balancing required to assess reasonable expectations of confidentiality will introduce some measure of unpredictability into the process.[334] This is undeniably a cost for suspects, judicial administration, and police departments trying to ascertain whether a search requires a warrant.[335] It is a cost that pervades much of the Fourth Amendment privacy analysis.[336] The present proposal would extend this uncertainty to the present predictability of third party cases. This a systemic issue that courts evaluating searches have to grapple with. At least so far as the present proposal is concerned, there some reason for relative optimism. Courts have a very long history and a good track record of assessing reasonable expectations of confidentiality in the privilege context. This long-standing jurisprudcence would be an aid to suspects, courts, and police navigating the early stages of Fourth Amendment confidentiality jurisprudence. Enforcement authorities with sufficiently well-founded suspicions can always secure a warrant and the assurances it brings.

These uncertainty costs of moving from privacy-as-secrecy to privacy-as-confidentiality should not be trivialized. However, where the options are between a rule that systematically undermines Fourth Amendment interests and a less efficient standard that has a chance of protecting them, the costs are easier to justify. Marginal inefficiencies in the courtroom and the police station are a small cost to pay for guarding our basic civil liberties. This is what thinking of privacy as confidentiality promises to do.

---

334 *See generally* Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992).

335 *See* Kerr, *supra* note 22, at 583–84.

336 *See* Christie v. Borough of Folcroft, No. Civ.A. 04-5944, 2005 WL 2396762, at *9 (E.D. Pa. Sept. 27, 2005) ("Analysis of [reasonable expectations of privacy] is fact-specific."); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 525–26 (2007) ("Fourth Amendment cases always involve a specific set of facts, and the policy model requires courts to imagine those facts as one example of a broader category of cases. But the choice of category is completely arbitrary: courts can pick along a continuum from extremely specific to very broad, and no point along the continuum is clearly better than another.").